Алгебра. Подготовка к экзамену.

q

June 26, 2021

Contents

1 «Алгебра, часть II»

1.1 1.Кольцо многочленов R[x] над областью целостности R. Теорема Безу. Теорема о числе корней многочлена. Формулы Виета.

§16 Многочлены

п. 1 Кольцо многочленов $K[x]$

Пусть K — область целостности, т.е. коммутативное кольцо с единицей и без делителей нуля. (например, $K = \mathbb{Z}$ — кольцо целых чисел)

Опр. Многочленом от переменной x с коэффициентами из K называется формальное выражение вида

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n$$

где n — целое неотрицательное число, $a_0, a_1, \ldots, a_n \in K$ — коэффициенты мн-на $f(x)$

(a_i называется коэф. многочлена $f(x)$ при x^i)

Опр. Два многочлена $f(x)$ и $g(x)$ считаются равными, если они имеют одинаковые коэффициенты при одинаковых степенях переменной x (с точностью до первых коэффициентов):

$$1 + 1x + 0x^2 \text{ и } 1 + 1x$$

формально различаются, но считаются равными

__Опр.__ Степенью многочлена $f(x)$ называется наибольшее число k такое, что $a_k \neq 0$, и обозн $\deg f(x)$

__Опр.__ Нулевым многочленом наз. многочлен, все коэффициенты к-рого — нули.

Нулевой многочлен обозначается 0

Мн-во всех многочленов $f(x)$ от переменной x с коэффициентами из области целостности K обозначается $K[x]$

Введем операции сложения и умножения на мн-ве $K[x]$

__Опр__ Суммой многочленов $f(x)$ и $g(x) \in K[x]$,

$$f(x) = \sum_i a_i x^i \qquad g(x) = \sum_i b_i x^i \quad (*)$$

называется многочлен $h_1(x) \in K[x]$

$$h_1(x) = \sum_i c_i x^i$$

где $c_i = a_i + b_i$ для всех i

__Опр__ Произведением многочленов $f(x), g(x) \in K[x]$ вида $(*)$ наз. многочлен $h_2(x) \in K[x]$

$$h_2(x) = \sum_k d_k x^k$$

где $d_k = \sum_{i+j=k} a_i b_j$

__Теорема 1__

По отношению к введенным операциям сложения и умножения мн-во $K[x]$ является областью целостности и называется кольцом многочленов от переменной x с коэффициентами из K.

__Доказательство.__

Нулевой многочлен — нулевой эл-нт $K[x]$;

многочлен $f(x) = 1$, где 1 - единичный эл-нт K, играет роль единичного эл-нта $K[x]$

Проверка ассоциативности умножения, его коммутативности, а также проверка дистрибутивности умножения отн. сложения проводится на основе определений операций сложения, умножения и соответствующих св-в кольца коэф. K

Докажем, что если $f(x) \neq 0 \neq g(x)$, то $h(x) = f(x) \cdot g(x) \neq 0$, т.е. в кольце $K[x]$ нет делителей нуля

Действительно, имеем

$$\deg h(x) = \deg f(x) + \deg g(x) \quad (**)$$

что следует из отсутствия делителей нуля в K. - коэф. перед наиб. степенью не сократ.

Итак, $K[x]$ - область целостности.

<u>Замечание</u>

Утверждение теоремы вполне очевидно для $\mathbb{R}[x]$ (по модулю формулы $(**)$).

<u>Опр</u> Говорят, что многочлен $f(x) \in K[x]$ делится на $g(x) \in K[x]$, если существует $h(x) \in K[x]$, что $f(x) = g(x)\, h(x)$.

Легко видеть, что отношение делимости на мн-ве $K[x]$ обладает следующими св-вами:

1. Рефлексивность

   $f(x)$ делится на $f(x)$

2. Транзитивность

   Если $f(x)$ делится на $g(x)$, а $g(x)$ делится на $h(x)$, то $f(x)$ делится на $h(x)$.

<u>Опр</u> Пусть $f(x) \in K[x]$, $a \in K$

Разделить $f(x)$ на двучлен $x-a$ — это значит представить $f(x)$ в виде

$$f(x) = (x-a)\,q(x) + r$$

где $q(x) \in K[x]$, $r \in K$.

Опр. Векторы $x, y \in V$ называются ортогональными, если $(x, y) = 0$.

Опр. Система векторов $a_1, \ldots, a_m$ пр-ва V наз. ортогональной, если

$$(a_i, a_j) = 0 \text{ при } i \neq j, \; i, j = (1, \ldots, m).$$

Теорема 1

Ортогональная система векторов, не содержащая нулевых векторов, является линейно независимой.

Доказательство:

Пусть векторы $a_1, \ldots, a_m$ отличны от нулевого и образуют ~~.......~~ьную систему.

Докажем их линейную независимость.

Пусть $k_1 a_1 + \ldots + k_m a_m = 0$. Докажем, что, например, $k_1 = 0$.

Умножим скалярно обе части рав-ва на a_1

$$0 = (k_1 a_1 + k_2 a_2 + \ldots + k_m a_m, a_1) =$$
$$= k_1 (a_1, a_1) + k_2 \overset{\text{ортогон.}}{(a_2, a_1)}^{=0} + \ldots + k_m \overset{\text{ортогон.}}{(a_m, a_1)}^{=0} =$$
$$= k_1 (a_1, a_1)$$

По св-ву положит-ти т.к. $a_1 \neq 0$, $(a_1, a_1) > 0$, след-но $k_1 = 0$.

п. 2 Евклидово пространство

Опр. Конечномерное векторное пр-во V над полем $\mathbb{R}$, в к-ром задано нек-рое скалярное умножение векторов, называется Евклидовым пространством

Теорема 2

Любое конечномерное векторное пр-во V над полем F можно превратить в евклидово пространство.

Доказательство

Пусть $\dim V = n$, $b_1, \ldots, b_n$ — нек-рый базис V

Формула $(x, y) = x_1 y_1 + \ldots + x_n y_n$ (где $\begin{pmatrix} x_1 \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ y_n \end{pmatrix}$) — столбцы координат векторов x, y в данной

1.2 2. Алгебраическое и функциональное равенство многочленов. Интерполяционная формула Лагранжа.

многочлен $f(x) = 1$, где 1 - единичный эл-нт K, играет роль единичного эл-нта $K[x]$

Проверка ассоциативности умножения, его коммутативности, а также проверка дистрибутивности умножения отн. сложения проводится на основе определений операций сложения, умножения и соответствующих св-в кольца коэф. K

Докажем, что если $f(x) \neq 0 \neq g(x)$, то $h(x) = f(x) \cdot g(x) \neq 0$, т.е. в кольце $K[x]$ нет делителей нуля

Действительно, имеем

$$\deg h(x) = \deg f(x) + \deg g(x) \quad (**)$$

что следует из отсутствия делителей нуля в K. - коэф. перед наиб. степенью не сократ.

Итак, $K[x]$ - область целостности.

<u>Замечание</u>

Утверждение теоремы вполне очевидно для $\mathbb{R}[x]$ (по модулю формулы $(**)$).

<u>Опр</u> Говорят, что многочлен $f(x) \in K[x]$ делится на $g(x) \in K[x]$, если существует $h(x) \in K[x]$, что $f(x) = g(x) \cdot h(x)$.

Легко видеть, что отношение делимости на мн-ве $K[x]$ обладает следующими св-вами:

1. Рефлексивность

   $f(x)$ делится на $f(x)$

2. Транзитивность

   Если $f(x)$ делится на $g(x)$, а $g(x)$ делится на $h(x)$, то $f(x)$ делится на $h(x)$.

<u>Опр</u> Пусть $f(x) \in K[x]$, $a \in K$

Разделить $f(x)$ на двучлен $x-a$ — это значит представить $f(x)$ в виде

$$f(x) = (x-a)q(x) + r$$

где $q(x) \in K[x]$, $r \in K$.

Деление на $x-a$ осуществляется при помощи схемы Горнера

Пусть

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

Будем искать $q(x)$ в виде

$$q(x) = b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \ldots + b_1 x + b_0$$

методом неопределенных коэффициентов

Имеем:

$$a_n x^n + \ldots + a_1 x + a_0 = (x-a)(b_{n-1} x^{n-1} + \ldots + b_1 x + b_0) + r =$$
$$= b_{n-1} x^n + (b_{n-2} - a b_{n-1}) x^{n-1} + \ldots + (b_0 - a b_1) x + (r - a b_0)$$

Таким образом, для определения неизвестного коэффициентов b_i $(i = 1, \ldots, n-1)$ и r получаем систему равенств систему рав-в:

$$\begin{cases} a_n = b_{n-1} \\ a_{n-1} = b_{n-2} - a b_{n-1} \\ \ldots \\ a_1 = b_0 - a b_1 \\ a_0 = r - a b_0 \end{cases}$$

Отсюда находим (единственным образом)

$$\left.\begin{array}{l} b_{n-1} = a_n \\ b_{n-2} = a_{n-1} + a b_{n-1} \\ \ldots \\ b_0 = a_1 + a b_1 \end{array}\right\} \text{коэффициенты неполного частного } q(x)$$

$$r = a_0 + a b_0 \qquad \text{остаток от деления}$$

Вычисление коэффициентов неполного качества и остатка по указанным формулам реализуют в виде схемы Горнера.

<u>Пример</u>

$$K = \mathbb{R} \qquad f(x) = 2x^4 + 3x^3 - 2x^2 + 1 \qquad a = -1$$

$$\begin{array}{c|ccccc} & 2 & 3 & -2 & 0 & 1 \\ \hline -1 & \underbrace{2 \quad 1 \quad -3 \quad 3}_{q(x)} & & & & \underbrace{-2}_{r} \end{array}$$

$$f(x) = (x+1)(2x^3 + x^2 - 3x + 3) - 2$$

Из сказанного выше следует, что деление с остатком на двучлен $x-a$ всегда возможно, причем единственным образом

<u>Опр</u> Пусть $f(x) \in K[x]$

Элемент $a \in K$ является корнем многочлена $f(x)$, если $f(a) = 0$

<u>Замечание</u>

Если $a \in K$, то символом $f(a)$ обозначается результат подстановки в выражение $f(x)$ вместо формальной переременной x ее значение a:

$$f(a) = a_n a^n + a_{n-1} a^{n-1} + \ldots + a_1 a + a_0 \in K$$

Если $K \subset L$, то, очевидно, $K[x] \subset L[x]$. Поэтому можно говорить о корнях многочлена $f(x) \in K[x]$, принадлежащих L

<u>Теорема 2</u> (теорема Безу)

Многочлен $f(x) \in K[x]$ делится на $x - a \Leftrightarrow f(a) = 0$, т.е. a-корень $f(x)$

<u>Доказательство</u>

Разделим $f(x)$ на $x-a$ с остатком

$$f(x) = (x-a)q(x) + r$$

Подставив в это равенство $x = a$, получим:

$$0 = f(a) = r$$

<u>Опр.</u> Корень $a \in K$ многочлена $f(x) \in K[x]$ называется k-кратным, если $f(x)$ делится на $(x-a)^k$, но не делится на $(x-a)^{k+1}$

Корни кратности 1 называются простыми, остальные корни называются кратными.

Опр. Векторы $x, y \in V$ называются ортогональными, если $(x, y) = 0$.

Опр. Система векторов $a_1, \dots, a_m$ пр-ва V наз. ортогональной, если

$$(a_i, a_j) = 0 \text{ при } i \neq j, \quad i, j = (1, \dots, m).$$

Теорема 1

Ортогональная система векторов, не содержащая нулевых векторов, является линейно независимой

Доказательство:

Пусть векторы $a_1, \dots, a_m$ отличны от нулевого и образуют ~~…~~ьную систему.

Докажем их линейную независимость

Пусть $k_1 a_1 + \dots + k_m a_m = 0$ Докажем, что, например, $k_1 = 0$.

Умножим скалярно обе части рав-ва на a_1

$$0 = (k_1 a_1 + k_2 a_2 + \dots + k_m a_m, a_1) =$$
$$= k_1 (a_1, a_1) + k_2 \overset{\text{ортогон.}}{(a_2, a_1)}^{=0} + \dots + k_m \overset{\text{ор-огон.}}{(a_m, a_1)}^{=0} =$$
$$= k_1 (a_1, a_1)$$

По св-ву положит-ти т.к $a_1 \neq 0$, $(a_1, a_1) > 0$, след-но $k_1 = 0$.

п. 2 Евклидово пространство

Опр. Конечномерное векторное пр-во V над полем $\mathbb{R}$, в к-ром задано нек-рое скалярное умножение векторов, называется Евклидовым пространством

Теорема 2

Любое конечномерное векторное пр-во V над полем F можно превратить в евклидово пространство.

Доказательство

Пусть $\dim V = n$, $b_1, \dots, b_n$ — нек-рый базис V

Формула $(x, y) = x_1 y_1 + \dots + x_n y_n$ (где $\begin{pmatrix} x_1 \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ y_n \end{pmatrix}$ — столбцы координат векторов x, y в данном базисе) задает скалярное умножение в V.

Пусть V – евклидово пр-во, $\dim V = n$

<u>Опр.</u> Матрицей Грама скалярного произведения в базисе $b_1, .., b_n$ евклидова пр-ва V наз. матрица $G = (g_{ij})$, где $g_{ij} = (b_i, b_j)$, $i, j = 1, \dots, n$

<u>Опр</u> Базис называется ортогональным, если G – диагональная матрица, т.е. базис является ортогональной системой

<u>Опр.</u> Базис называется ортонормированным, если $G = E$ – единичная матрица

<u>Доказательство</u>

Пусть G – матрица Грама скалярного произведения в базисе $b_1, \dots, b_n$, а векторы $x, y \in V$ заданы своими координатами $x_1, \dots, x_n$ и $y_1, \dots, y_n$ в этом базисе.

Вычислим скалярное произведение этих векторов

$$(x, y) = (x_1 b_1 + \dots + x_n b_n, y_1 b_1 + \dots + y_n b_n) =$$
$$= \sum_{i,j=1}^{n} (x_i b_i, y_j b_j) = \sum_{i,j=1}^{n} x_i y_j (b_i, b_j) =$$
$$= \sum_{i,j=1}^{n} x_i y_j g_{ij} = (x_1 \dots x_n) G \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

В частности, если базис ортонормированный, т.е. $G = E$, то $(x, y) = (x_1 \dots x_n) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = x_1 y_1 + \dots + x_n y_n$

Пусть T – матрица перехода от базиса $b_1, .., b_n$ к базису $b_1', \dots, b_n'$, $T = (t_{ij})$

Имеем:

$$(b_i'; b_j') = \left(\sum_{k=1}^{n} t_{ki} b_k, \sum_{l=1}^{n} t_{lj} b_l\right) =$$
$$= \sum_{k,l=1}^{n} t_{ki} t_{lj} (b_k, b_l) = \sum_{k,l=1}^{n} t_{ki} g_{kl} t_{lj}$$

Отсюда:

$$G' = T^t G T$$

1.3 3. Кольцо многочленов F[x] над полем F. Деление с остатком. Наибольший общий делитель многочленов.

$$
\begin{array}{c|ccccc}
 & 2 & 3 & -2 & 0 & 1 \\
\hline
-1 & \underbrace{2 \quad 1 \quad -3 \quad 3}_{q(x)} & & & & \underbrace{-2}_{r}
\end{array}
$$

$$f(x) = (x+1)(2x^3 + x^2 - 3x + 3) - 2$$

Из сказанного выше следует, что деление с остатком на двучлен $x-a$ всегда возможно, причем единственным образом

Опр. Пусть $f(x) \in K[x]$

Элемент $a \in K$ является корнем многочлена $f(x)$, если $f(a) = 0$

Замечание

Если $a \in K$, то символом $f(a)$ обозначается результат подстановки в выражение $f(x)$ вместо формальной переменной x ее значение a:

$$f(a) = a_n a^n + a_{n-1} a^{n-1} + \ldots + a_1 a + a_0 \in K$$

Если $K \subset L$, то, очевидно, $K[x] \subset L[x]$. Поэтому можно говорить о корнях многочлена $f(x) \in K[x]$, принадлежащих L

Теорема 2 (теорема Безу)

Многочлен $f(x) \in K[x]$ делится на $x - a \Leftrightarrow f(a) = 0$, т.е. a-корень $f(x)$

Доказательство

Разделим $f(x)$ на $x-a$ с остатком

$$f(x) = (x-a)\,q(x) + r$$

Подставив в это равенство $x = a$, получим:

$$0 = f(a) = r$$

Опр. Корень $a \in K$ многочлена $f(x) \in K[x]$ называется k-кратным, если $f(x)$ делится на $(x-a)^k$, но не делится на $(x-a)^{k+1}$

Корни кратности 1 называются простыми, остальные корни называются кратными.

Теорема 3 (о числе корней многочлена)

Пусть $f(x) \in K[x]$ и $n = \deg f(x) > 0$

Тогда число корней многочлена $f(x)$ с учетом их кратностей не превосходит n

Доказательство

Индукция по $n \geq 1$

База индукции очевидна. Предположим, что утверждение доказано для всех многочленов степени меньше n и пусть $f(x)$ – произвольный многочлен степени n

Докажем утверждения для многочлена $f(x)$
Если многочлен $f(x)$ не имеет корней, то доказывать нечего

Иначе многочлен $f(x)$ имеет некоторый корень $a \in K$ Пусть a – корень кратности $k \geq 1$, т.е

$$f(x) = (x-a)^k g(x)$$

причем $g(a) \neq 0$ и $\deg g(x) < \deg f(x)$

По предположению индукции число корней многочлена $g(x)$ с учетом их кратности не превосходит $\deg g(x)$.

Ясно, что корни многочлена $f(x)$ – элемент a и все корни многочлена $g(x)$ (следствие целостности кольца K (нет делителей нуля))

Теперь утверждение теоремы для многочлена $f(x)$ очевидно

Добавления к теореме 3

Если число корней с учетом кратности многочлена $f(x)$ равно $n = \deg f(x)$, то имеет место разложение:

$$f(x) = a_0 (x-a_1)^{k_1} \cdot \ldots \cdot (x-a_s)^{k_s} \quad (*)$$

где $a_0 \in K$, $a_0 \neq 0$
$a_1, \ldots, a_s$ – попарно различные корни $f(x)$, $s \geq 1$

Разложение $(*)$ можно записать в виде:

$$f(x) = a(x-x_1) \ldots (x-x_m) \quad (**)$$

где $a \in K$, $a \neq 0$,

$x_1, \quad , x_n$ – корни $f(x)$ (не обязательно различные)

Предполагая наличие разложения (**) получим так называемые формулы Виета

$$f(x) = a_n x^n + \quad + \; + a_1 x + a_0 = \; = a(x - x_1) \quad (x - x_n)$$

Раскрыв скобки в правой части, получим

$$a_n = a$$

$$a_{n-1} = a(-x - \quad - x_n)$$

$$a_{n-2} = \; = a(x_1 x_2 + \quad + x_{n-1} x_n)$$

$$a_{n-k} = \; = a(-1)^k \sum_{1 \le i_1 < \quad < i_k \le n} x_{i_1} \quad x_{i_k}$$

$$a_0 = a(-1)^n x_1 \quad x_n$$

Точнее, формулами Виета обычно называются формулы

$$\sum_{0 \le i_1 < \quad < i_k \le n} x_{i_1} \quad x_{i_k} = \; = (-1)^k \frac{a_{n-k}}{a_n}$$

$$1 \le k \le n$$

Замечание

Выражение, стоящее в левых частях формулы Виета, называется элементарными симметрическими многочленами от корней данного многочлена $f(x)$

Опр. Функцией определенной многочленом $f(x) \in K[x]$ называется функция

$$\tilde{f} \quad K \to K,$$

задаваемая правилом

$$a \to f(a),\ a \in K$$

Если $f(x) \neq g(x)$ в K[x], то, вообще говоря, функции, определяемые многочленами $f(x)$ и $g(x)$, могут совпадать

Пример

$K = F_2 = \{0,1\}$ – поле из 2 элементов

$f(x) = x + 1$

$g(x) = x^2 + 1$

Составим таблицы значений соответствующих функций

$f(x) = x + 1$		$g(x) = x^2 + 1$	
a	$f(a)$	a	$g(a)$
0	1	0	1
1	0	1	0

Теорема 4 (о совпадении алгебраической и функциональной точек зрения на понятие многочлена)

Пусть K – бесконечная область целостности

Тогда f (x) = g (x) $\Leftrightarrow \tilde{f} = \tilde{g}$

базисе) задает скалярное умножение в V.

Пусть V – евклидово пр-во, $\dim V = n$

Опр. Матрицей Грама скалярного произведения в базисе $b_1, .., b_n$ евклидова пр-ва V наз. матрица $G = (g_{ij})$, где $g_{ij} = (b_i, b_j)$, $i, j = 1, \dots, n$

Опр. Базис называется ортогональным, если G – диагональная матрица, т.е. базис является ортогональной системой

Опр. Базис называется ортонормированным, если $G = E$ – единичная матрица

Доказательство

Пусть G – матрица Грама скалярного произведения в базисе $b_1, \dots, b_n$, а векторы $x, y \in V$ заданы своими координатами $x_1, \dots, x_n$ и $y_1, \dots, y_n$ в этом базисе.

Вычислим скалярное произведение этих векторов

$$(x, y) = (x_1 b_1 + \dots + x_n b_n, y_1 b_1 + \dots + y_n b_n) =$$
$$= \sum_{i,j=1}^{n} (x_i b_i, y_j b_j) = \sum_{i,j=1}^{n} x_i y_j (b_i, b_j) =$$
$$= \sum_{i,j=1}^{n} x_i y_j g_{ij} = (x_1 \dots x_n)\, G \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

В частности, если базис ортонормированный, т.е. $G = E$, то $(x, y) = (x_1 \dots x_n)\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = x_1 y_1 + \dots + x_n y_n$

Пусть T – матрица перехода от базиса $b_1, .., b_n$ к базису $b_1', \dots, b_n'$, $T = (t_{ij})$

Имеем:

$$(b_i'; b_j') = \left(\sum_{k=1}^{n} t_{ki} b_k, \sum_{l=1}^{n} t_{lj} b_l\right) =$$
$$= \sum_{k,l=1}^{n} t_{ki} t_{lj} (b_k, b_l) = \sum_{k,l=1}^{n} t_{ki} g_{kl} t_{lj}$$

Отсюда:

$$G' = T^t G T$$

~~Итак~~

Для построения ортонормированных базисов используют процесс ортогонализации Грама–Шмидта

Теорема 3

В любом евклидовом пр-ве существуют ортонормированные базисы.

Доказательство

Пусть дана нек-рая линейно независимая система векторов $a_1, \ldots, a_m$ в евклидовом пр-ве V

Построим ортогональную систему ненулевых векторов $b_1, \ldots, b_m$, при этом

$$\langle b_1, \ldots, b_m \rangle = \langle a_1, \ldots, a_m \rangle$$

Положим $b_1 = a_1$ ($b_1 \neq 0$, т.к. по условию $a_1, \ldots, a_m$ линейно независимы)

Предположим, что уже построены векторы $b_1, \ldots, b_k$, обладающие нужными св-вами, т.е. $b_1, \ldots, b_k$ – система ортогональная ненулевых векторов и $\langle b_1, \ldots, b_k \rangle = \langle a_1, \ldots, a_k \rangle$

Покажем, как найти b_{k+1}. Положим

$$b_{k+1} = a_{k+1} - l_1 b_1 - \ldots - l_k b_k$$

где коэффициенты $l_1, \ldots, l_k$ найдены из условия

$$(b_{k+1}, b_i) = 0 \qquad i = 1, \ldots, k$$

т.е.

$$0 = (b_{k+1}, b_i) = (a_{k+1} - l_1 b_1 - \ldots - l_k b_k, b_i) =$$
$$= (a_{k+1}, b_i) - l_i (b_i, b_i) - 0 \quad \left(\text{т.к. } b_1, \ldots, b_k \text{ ортогональны, след-но их скаляр. произв. равно } 0\right)$$

отсюда

$$l_i = \frac{(a_{k+1}, b_i)}{(b_i, b_i)} \qquad i = 1, \ldots, k$$

Заметим, что $b_{k+1} \neq 0$. Иначе a_{k+1} есть нек-рая линейная комбинация $b_1, \ldots, b_k$, а значит, т.к. $\langle b_1, \ldots, b_k \rangle = \langle a_1, \ldots, a_k \rangle$, и векторов $a_1, \ldots, a_k$ – противоречие с линейной независимостью системы $a_1, \ldots, a_m$

Кроме того, $\langle b_1, \ldots, b_k, b_{k+1} \rangle = \langle a_1, \ldots, a_k, a_{k+1} \rangle$, что следует из рав-ва

$$\langle a_1, \dots, a_k \rangle = \langle b_1, \dots, b_k \rangle$$

а также из того, что

$$b_{k+1} = a_{k+1} - l_1 b_1 - \dots - l_k b_k$$

(т.к. a_{k+1} линейно выражается ч/з $b_1, \dots, b_k, b_{k+1}$)

В итоге получим ортогональную систему векторов $b_1, \dots, b_m$, обладающую требуемыми св-вами.

В частности, если $a_1, \dots, a_n$ — базис евклидова пр-ва V, то применение процесса ортогонализации к нему приводит к ортогональному базису $b_1, \dots, b_n$

Нормировкой вектора $b \in V$ называется его замена на вектор

$$\tilde{b} = \frac{b}{\sqrt{(b, b)}} \quad (b \neq 0)$$

Имеем $(\tilde{b}, \tilde{b}) = 1$

Отнормировав полученный ортогональный базис, получим ортонормированный базис $\tilde{b}_1, \dots, \tilde{b}_n$

Пример

Пусть $V = \mathbb{R}^3$, умножение стандартно скалярн

$$b_1 = a_1 = (1, -1, 2)$$

$$b_2 = a_2 - l b_1 \qquad l = \frac{(a_2, b_1)}{(b_1, b_1)} = \frac{3}{6} = \frac{1}{2}$$

$$b_2 = \left(-\frac{1}{2}, -\frac{1}{2}, 0\right)$$

$$b_3 = a_3 - k b_1 - f b_2 \qquad k = \frac{(a_3, b_1)}{(b_1, b_1)} = \frac{2}{6} = \frac{1}{3} \quad f = \frac{(a_3, b_2)}{(b_2, b_2)} = \frac{0}{1/2} = 0$$

$$b_3 = \left(-\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right)$$

$$\tilde{b}_1 = \frac{b_1}{\sqrt{(b_1, b_1)}} = \left(\frac{1}{\sqrt{6}}, -\frac{1}{\sqrt{6}}, \frac{2}{\sqrt{6}}\right)$$

$$\tilde{b}_2 = \frac{b_2}{\sqrt{(b_2, b_2)}} = \left(-\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2}, 0\right)$$

$$\tilde{b}_3 = \frac{b_3}{\sqrt{(b_3, b_3)}} = \left(-\frac{\sqrt{3}}{3}, \frac{\sqrt{3}}{3}, \frac{\sqrt{3}}{3}\right)$$

$\tilde{b}_1, \tilde{b}_2, \tilde{b}_3$ — ортонормированный базис.

Опр. Пусть L – подпр-во евклидова пр-ва V.
Ортогональным дополнением к L называется подпр-во:

$$L^{\perp} = \{ x \in V \mid (x,y) = 0 \quad \forall y \in L \}$$

Замечание

Ортогональное дополнение $L^{\perp}$ действительно является подпространством, т.к. это следует из характеристического признака подпространства

Теорема 4

1. Если $L_1 \subset L_2$, то $L_1^{\perp} \supset L_2^{\perp}$
2. $(L^{\perp})^{\perp} = L$
3. $(L_1 + L_2)^{\perp} = L_1^{\perp} \cap L_2^{\perp}$
4. $(L_1 \cap L_2)^{\perp} = L_1^{\perp} + L_2^{\perp}$
5. $V = L \oplus L^{\perp}$

L_1, L_2, L – подпр-ва евклидова пр-ва V

Доказательство

1. Непосредственно следует из определения ортогонального дополнения
2. Не трудно видеть, что $(L^{\perp})^{\perp} \supset L$

Пусть $\dim L = k$, $\dim V = n$

Из утверждения п. 5 следует, что $(L^{\perp})^{\perp} = \dim V - \dim L^{\perp} = n - (n-k) = k$

След-но $\dim L = \dim (L^{\perp})^{\perp}$. Тогда т.к. $L \subset (L^{\perp})^{\perp}$, то $L = (L^{\perp})^{\perp}$.

3. Пусть $x \in L_1^{\perp} \cap L_2^{\perp}$. Тогда $(x, y_1) = 0$ и $(x, y_2) = 0 \quad \forall y_1 \in L_1, y_2 \in L_2$

След-но $(x, \underbrace{y_1 + y_2}_{\in L_1 + L_2}) = 0$, т.е. x ортогонален

произвольному вектору из $L_1 + L_2$, т.е. $x \in (L_1 + L_2)^{\perp}$, след-но $L_1^{\perp} \cap L_2^{\perp} \subset (L_1 + L_2)^{\perp}$

Очевидно, пусть $x \in (L_1 + L_2)^{\perp}$, т.е. $(x,y) = 0$

$\forall y \in L_1 + L_2$. Тогда, в частности, это верно $\forall y \in L_1$ и $\forall y \in L_2$, т.е. $x \in L_1^\perp$ и $x_2 \in L_2^\perp$, а значит $x \in L_1^\perp \cap L_2^\perp$

4. Пусть $L_1^\perp = \tilde{L}_1$, $L_2^\perp = \tilde{L}_2$.

$$(L_1 + L_2)^\perp = \tilde{L}_1 \cap \tilde{L}_2$$

$$((L_1 + L_2)^\perp)^\perp = (\tilde{L}_1 \cap \tilde{L}_2)^\perp$$

$$L_1 + L_2 = (\tilde{L}_1 \cap \tilde{L}_2)^\perp$$

$$\tilde{L}_1^\perp + \tilde{L}_2^\perp = (\tilde{L}_1 \cap \tilde{L}_2)^\perp$$

5. Выберем в L некоторый базис $b_1, \dots, b_k$ и дополним его до базиса $b_1, \dots, b_k, b_{k+1}, \dots, b_n$ пр-ва V.

Применим к этому базису $b_1, \dots, b_n$ процесс ортогонализации. Получим ортогональный базис $b_1', \dots, b_n'$

Имеем:

$L = \langle b_1, \dots, b_k \rangle = \langle b_1', \dots, b_k' \rangle$,

$L^\perp = \langle b_{k+1}', \dots, b_n' \rangle$ (т.к. $b_{k+1}', \dots, b_n'$ ортогон. $b_1', \dots, b_k'$ и всякий вектор из V расклад. по $b_1', \dots, b_n'$)

Очевидно, что $L \oplus L^\perp = V$

1.4 4. Алгоритм Евклида. Линейная форма наибольшего общего делителя многочленов.

где $a \in K,\ a \neq 0,$

$x_1, \quad , x_n$ – корни $f(x)$ (не обязательно различные)

Предполагая наличие разложения (**) получим так называемые формулы Виета

$$f(x) = a_n x^n + \quad + \ + a_1 x + a_0 = \ = a(x - x_1) \quad (x - x_n)$$

Раскрыв скобки в правой части, получим

$$a_n = a$$

$$a_{n-1} = a(-x - \quad - x_n)$$

$$a_{n-2} = \ = a(x_1 x_2 + \quad + x_{n-1} x_n)$$

$$a_{n-k} = \ = a(-1)^k \sum_{1 \le i_1 < \quad < i_k \le n} x_{i_1} \quad x_{i_k}$$

$$a_0 = a(-1)^n x_1 \quad x_n$$

Точнее, формулами Виета обычно называются формулы

$$\sum_{0 \le i_1 < \quad < i_k \le n} x_{i_1} \quad x_{i_k} = \ = (-1)^k \frac{a_{n-k}}{a_n}$$

$$1 \le k \le n$$

Замечание

Выражение, стоящее в левых частях формулы Виета, называется элементарными симметрическими многочленами от корней данного многочлена $f(x)$

Опр. Функцией определенной многочленом $f(x) \in K[x]$ называется функция

$$\tilde{f} \quad K \to K,$$

задаваемая правилом

$$a \to f(a),\ a \in K$$

Если $f(x) \neq g(x)$ в K[x], то, вообще говоря, функции, определяемые многочленами $f(x)$ и $g(x)$, могут совпадать

Пример

$K = F_2 = \{0,1\}$ – поле из 2 элементов

$f(x) = x + 1$

$g(x) = x^2 + 1$

Составим таблицы значений соответствующих функций

$f(x) = x + 1$		$g(x) = x^2 + 1$	
a	$f(a)$	a	$g(a)$
0	1	0	1
1	0	1	0

Теорема 4 (о совпадении алгебраической и функциональной точек зрения на понятие многочлена)

Пусть K – бесконечная область целостности

Тогда f (x) = g (x) $\Leftrightarrow \tilde{f} = \tilde{g}$

Доказательство

Неочевидным является доказательство утверждения если $\tilde{f} = \tilde{g}$, то $f(x) = g(x)$ (в K[x])

Рассуждаем от противного Пусть $f(x) \neq g(x)$ Рассмотрим $h(x) = f(x) - g(x) \neq 0$

deg $h(x)$ определена

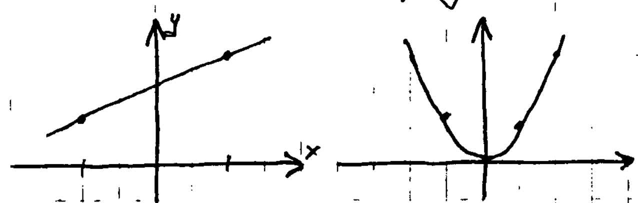
Так как $\tilde{f}(a) = \tilde{g}(a)$ $\forall a \in K$, то $h(a) = 0$ $\forall a \in K$

Но число корней многочлена h (x) конечно (не превосходит deg $h(x)$) – противоречие, доказывающее утверждение

Замечание

Фактически доказано следующее утверждение: если многочлены $f(x)$ и $g(x) \in K[x]$ степени n-рых не превосходит и совпадают при $x = a_i$, где $i = 1, \ldots, n+1$; при этом $a_1, \ldots, a_{n+1}$ попарно различны, то $f(x) = g(x)$ в $K[x]$.

Другими словами, существует не более одного многочлена степени не выше n, к-рый принимает в данных $n+1$ различных точках предписанные значения.



$n = 1$ $\quad$ $n = 2$

В общем случае существование такого многочлена не гарантируется.

Предположим теперь, что $K = F$ — поле. Тогда многочлен, о к-ром шла речь в замечании, всегда существует. Он может быть найден по интерполяционной формуле Лагранжа.

Пусть b_i — предписанные значения многочлена $f(x)$ в точках $x = a_i$ $(i = 1, \ldots, n+1)$. Тогда многочлен $f(x)$ находится из формулы

$$f(x) = \sum_{i=1}^{n+1} \frac{(x-a_1)\cdot\ldots\cdot(x-a_{i-1})(x-a_{i+1})\cdot\ldots\cdot(x-a_{n+1})}{(a_i-a_1)\cdot\ldots\cdot(a_i-a_{i-1})(a_i-a_{i+1})\cdot\ldots\cdot(a_i-a_{n+1})}\, b_i$$

$\forall y \in L_1 + L_2$. Тогда, в частности, это верно $\forall y \in L_1$ и $\forall y \in L_2$, т.е. $x \in L_1^\perp$ и $x_2 \in L_2^\perp$, а значит $x \in L_1^\perp \cap L_2^\perp$

4. Пусть $L_1^\perp = \tilde{L}_1$, $L_2^\perp = \tilde{L}_2$.

$$(L_1 + L_2)^\perp = \tilde{L}_1 \cap \tilde{L}_2$$
$$((L_1+L_2)^\perp)^\perp = (\tilde{L}_1 \cap \tilde{L}_2)^\perp$$
$$L_1 + L_2 = (\tilde{L}_1 \cap \tilde{L}_2)^\perp$$
$$\tilde{L}_1^\perp + \tilde{L}_2^\perp = (\tilde{L}_1 \cap \tilde{L}_2)^\perp$$

5. Выберем в L нек-рый базис $b_1, \ldots, b_k$ и дополним его до базиса $b_1, \ldots, b_k, b_{k+1}, \ldots, b_n$ пр-ва V.

Применим к этому базису $b_1, \ldots, b_n$ процесс ортогонализации. Получим ортогональный базис $b_1', \ldots, b_n'$

Имеем:

$L = \langle b_1, \ldots, b_k \rangle = \langle b_1', \ldots, b_k' \rangle$,

$L^\perp = \langle b_{k+1}', \ldots, b_n' \rangle$ (т.к. $b_{k+1}', \ldots, b_n'$ ортогон. $b_1', \ldots, b_k'$ и всякий вектор из V расклад. по $b_1', \ldots, b_n'$)

Очевидно, что $L \oplus L^\perp = V$

1.3 Геометрия евклидова пространства

Теорема 5 (неравенство Коши–Буняковского)

Пусть V – евклидово пр-во, $\dim V = n$. Тогда

$(a, b)^2 \leq (a, a) \cdot (b, b)$ $\forall a, b \in V$, причем равенство имеет место тогда и только тогда, когда a и b линейно зависимы (пропорциональны).

Доказательство

Если $b = 0$, то нер-во очевидно.

Будем считать, что $b \neq 0$. Рассмотрим вектор

$$x = a + t\, b$$

где $t \in \mathbb{R}$

Имеем

$$0 \leq (x, x) = (a + tb, a + tb) = (a, a) + 2abt + (b, b)t^2 = f(t)$$

$$D = 4(a,b)^2 - 4(a,a)(b,b) \le 0 \Rightarrow (a,b)^2 \le (a,a)(b,b)$$

Следствие 1

$$|(a,b)| \le \sqrt{(a,a)} \cdot \sqrt{(b,b)} \quad (*)$$

Опр Длиной вектора $a \in V$ называется величина $\sqrt{(a,a)}$

Обозначение $|a|$

Следствие 2 (нер-во треугольника)

$$|a+b| \le |a| + |b|$$

Доказательство

$$|a+b| \le |a| + |b| \Leftrightarrow |a+b|^2 \le |a|^2 + 2|ab| + |b|^2$$

$$(a+b, a+b) \le (a,a) + 2|a||b| + (b,b)$$

$$(a,a) + 2(a,b) + (b,b) \le (a,a) + 2|a||b| + (b,b)$$

$$(a,b) \le |a|\,|b| = \sqrt{(a,a)}\sqrt{(b,b)}$$

Это нер-во явл. следствием нер-ва $(*)$

Опр Пусть векторы $a, b \in V$ ненулевые

Угол φ м/у этими векторами определяется из рав-ва

$$\cos\varphi = \frac{(a,b)}{|a||b|}$$

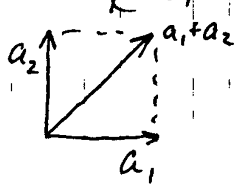
Замечание

Это определение корректно, т.к. $\left|\frac{(a,b)}{|a||b|}\right| \le 1$ по Следствию 1. Теоремы 5.

Теорема 6 (теорема Пифагора)

Пусть векторы $a_1, \dots, a_m$ образуют ортогональную систему. Тогда:

$$|a_1 + \dots + a_m|^2 = |a_1|^2 + \dots + |a_m|^2$$



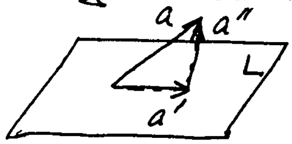
Доказательство

$$|a_1 + .. + a_m|^2 = (a_1 + .. + a_m, a_1 + .. + a_m) =$$

$= (a_1, a_1) + \ldots + (a_m, a_m) = |a_1|^2 + \ldots + |a_m|^2$

Пусть L — подпр-во V, $a \in V$. Имеем $V = L \oplus L^{\perp}$, след-но $a = a' + a''$, $a' \in L$, $a'' \in L^{\perp}$

Здесь a'' — так называемая ортогональная составляющая вектора a, a' — ортогональная проекция a на L



Пусть L — подпр-во V, $a \in V$

Угол φ м/у a и L определяется из рав-ва

$$\cos\varphi = \max_{0 \neq b \in L} \frac{(a,b)}{|a||b|} = \frac{|a'|}{|a|}$$

где a' — ортогональная проекция a на L.

<u>Опр.</u> Пусть L_1, L_2 — подпр-ва V

Если $L_1 \cap L_2 = \{0\}$, то угол φ м/у L_1 и L_2 определяется рав-вом:

$$\cos\varphi = \max_{\substack{0 \neq a \in L_1 \\ 0 \neq b \in L_2}} \frac{(a,b)}{|a||b|}$$

иначе $L = L_1 \cap L_2 \neq \{0\}$ и углом м/у L_1 и L_2 считается угол м/у $L_1 \cap L^{\perp}$ и $L_2 \cap L^{\perp}$

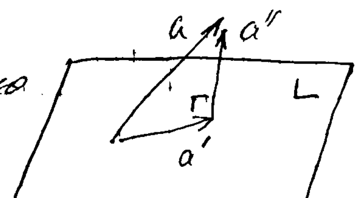
<u>Замечание</u>

Можно показать, что $(L_1 \cap L^{\perp}) \cap (L_2 \cap L^{\perp}) = \{0\}$.

Нахождение ортогональной проекции и орт. составл. вектора

Пусть $L = \langle b_1, \ldots, b_k \rangle$, $b_1, \ldots, b_k$ линейно независимы

Ортогональную проекцию можно представить в виде



$$a' = x_1 b_1 + \ldots + x_n b_n$$

Где коэффициенты $x_1, \ldots, x_n$ подлежат определению

Имеем:

$$a'' = a - a' = a - x_1 b_1 - \quad - x_k b_k$$

ортогонален векторам $b_1, \ldots, b_k$, т.е.

Экстремальное свойство ортогональной составляющей. $\min\limits_{b \in L} |a-b| = |a-a'| = |a''|$.

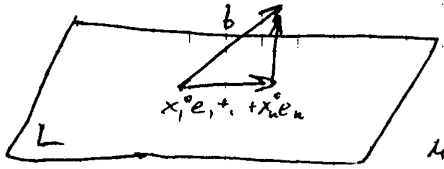
<u>Доказательство</u> Имеем $|a-b|^2 = |a-a'+a'-b|^2 =$
$= |a''+(a'-b)|^2 = |a''|^2 + |a'-b|^2 \geqslant |a''|^2$,
причем равенство возможно только при $b=a'$. $\square$

Докажем, что $\max\limits_{0 \neq b \in L} \frac{(a,b)}{|a|\cdot|b|} = \frac{|a'|}{|a|}$. Пусть $a' \neq 0$.

Имеем $\frac{(a,b)}{|a|\cdot|b|} = \frac{(a'+a'',b)}{|a|\cdot|b|} = \frac{(a',b)}{|a|\cdot|b|} \leqslant$
$\leqslant \frac{|a'|\cdot|b|}{|a|\cdot|b|} = \frac{|a'|}{|a|}$, причем равенство возможно только при $b = ka'$, где $k>0$

$$x_1 e_1 + \ldots + x_n e_n = b$$

$$\sqrt{\sum_{i=1}^{n}\left(\sum_{j=1}^{m} a_{ij} x_j^0 - b_i\right)^2} = \left|x_1^0 e_1 + \ldots + x_n^0 e_n - b\right|$$



Графическое представление ситуации при наименьшем среднеквадратичном отклонении

$L = \langle e_1, \ldots, e_n \rangle$, $\dim L = n$

Наименьшее среднеквадратичное отклонение будет в том случае, когда в качестве $x_1^0, \ldots, x_n^0$ взяты координаты ортогональных проекции вектора b на подпространство $L = \langle e_1, \ldots, e_n \rangle$

<u>Опр</u> Пусть даны векторы $b_1, \ldots, b_n$ в n-мерном евклидовом пр-ве V

Предположим, что они линейно независимы и заданы своими координатами

$\begin{pmatrix} t_{11} \\ \ldots \\ t_{n1} \end{pmatrix}, \ldots, \begin{pmatrix} t_{1n} \\ \ldots \\ t_{nn} \end{pmatrix}$ в нек-ром ортонормированном базисе.

Тогда объем параллелепипеда $\Pi(b_1, \ldots, b_n) = \{x_1 b_1 + \ldots + x_n b_n \mid 0 \le x_i \le 1,\ i = 1, \ldots, n\}$, натянутого на векторы $b_1, \ldots, b_n$ наз число

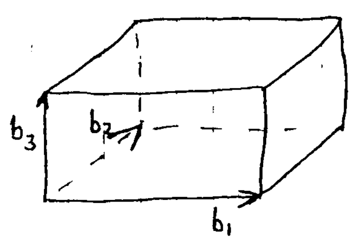
$$|\det(T)|$$

где

$$T = \begin{pmatrix} t_{11} & \ldots & t_{1n} \\ \ldots & \ldots & \ldots \\ t_{n1} & \ldots & t_{nn} \end{pmatrix}$$

<u>Пример</u>

Пусть $b_1, \ldots, b_n$ — ортогональный базис евклидова пр-ва V



В качестве ортонормированного базиса возьмем тот, к-рый получается нормировкой базиса $b_1, \ldots, b_n$.

Тогда матрица T примет вид:

$$T = \begin{pmatrix} |b_1| & 0 & \dots & 0 \\ 0 & |b_2| & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & |b_n| \end{pmatrix}$$

След-но

$$V = |\det T| = |b_1| |b_2| \cdot \ldots \cdot |b_n|$$

Теорема 7

Объем параллелепипеда $\Pi(b_1, .., b_n)$ равен

$$\sqrt{\det(G(b_1, \dots, b_n))}$$

где $G(b_1, \dots, b_n)$ – матрица Грама скалярного произведения в базисе $b_1, \dots, b_n$, т.е.

$$G = \begin{pmatrix} (b_1, b_1) & \dots & (b_1, b_n) \\ \dots & \dots & \dots \\ (b_n, b_1) & \dots & (b_n, b_n) \end{pmatrix}$$

Замечание

Отсюда следует, в частности, корректность определения объема параллелепипеда, т.е. независимость от выбора ортонормированного базиса

Доказательство

Пусть $e_1, \dots, e_n$ – тот ортонормированный базис, о к-ром идет речь в определении объема

Тогда матрица T – это матрица перехода от базиса $e_1, .., e_n$ к базису $b_1, \dots, b_n$

Имеем:

$$G = T^t \cdot E \cdot T$$

Перейдем к определителям:

$$\det G = \det(T^t T) = \det(T^t) \cdot \det(T) = (\det T)^2$$

Извлекая квадратный корень из обоих частей равенства получим доказываемое выражение

1.5 2. Взаимно простые многочлены и их свойства. Наименьшее общее кратное многочленов.

п. 3 Кольцо многочленов $F[x]$ над полем F

Опр. Пусть $f(x), g(x) \in F[x]$, $g(x) \neq 0$

Разделить $f(x)$ на $g(x)$ с остатком – это значит представить $f(x)$ в виде:

$$f(x) = g(x) \cdot q(x) + r(x)$$

где $q(x), r(x) \in F[x]$

$q(x)$ – неполное частное

$r(x)$ – остаток

при этом либо $r(x) = 0$, либо $\deg r(x) < \deg g(x)$

Теорема 5

Деление с остатком всегда возможно в $F[x]$ и притом единственным образом.

Доказательство

1. Существование

Неполное частное $q(x)$ и остаток $r(x)$ находятся при помощи процедуры „деления уголком".

Продемонстрируем это на примере. Пусть

$$f(x) = 4x^3 - 2x^2 + x - 1$$

$$g(x) = x^2 - x + 1$$

(здесь $F = \mathbb{R}$)

$$\begin{array}{r|l}
-\,4x^3 - 2x^2 + x - 1 & x^2 - x + 1 \\
\cline{2-2}
\underline{4x^3 - 4x^2 + 4x} \quad & 4x + 2 \quad = q(x) \\
-\,2x^2 - 3x - 1 & \\
\underline{2x^2 - 2x + 2} & \\
x - 3 \; = r(x) &
\end{array}$$

2. Единственность

Пусть $f(x) = g(x)q_1(x) + r_1(x) = g(x)q_2(x) + r_2(x)$ — два способа поделить $f(x)$ на $g(x)$ с остатком.

Имеем:

$$g(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x)$$

Если допустить, что $q_1(x) \neq q_2(x)$, то $r_2(x) - r_1(x) \neq 0$ и $\deg(r_2(x) - r_1(x)) < \deg g(x)$,

$$\deg(g(x)(q_1(x) - q_2(x))) \geq \deg g(x) > \deg(r_1(x) - r_2(x))$$

противоречие, след-но $q_1(x) = q_2(x)$ и $r_1(x) = r_2(x)$.

Опр. Пусть $f_1(x), \ldots, f_m(x) \in F[x]$ — многочлены, среди к-рых есть отличные от 0

Наибольшим общим делителем (НОД) этих многочленов называется любой многочлен $d(x) \in F[x]$, обладающий следующими свойствами:

1. $f_1(x), \ldots, f_m(x)$ делятся на $d(x)$, т.е. $d(x)$ есть общий делитель $f_1(x), \ldots, f_m(x)$.
2. Если $d_1(x)$ — любой другой общий делитель многочленов $f_1(x), \ldots, f_m(x)$, то $d(x)$ делится на $d_1(x)$.

Аналогично определяется наименьшее общее кратное (НОК) ненулевых многочленов $f_1(x), \ldots, f_m(x)$: слово „делитель" заменяется на „кратное".

Равенство вида

$$d(x) = \text{НОД}\,(f_1(x), \ldots, f_m(x))$$

означает, что многочлен $d(x)$ является одним из НОД многочленов $f_1(x), \ldots, f_m(x)$.

Аналогично следует понимать равенство

$$m(x) = \text{НОК}\,(f_1(x), \ldots, f_m(x))$$

<u>Замечание</u>

1. Из определений формально не следует, что НОД и НОК данных многочленов существуют.

   На самом деле, как будет показано ниже, они существуют.

2. Если $d(x)$ некоторый НОД многочленов $f_1(x), \ldots, f_m(x)$, то любой другой НОД этих многочленов $\tilde{d}(x)$ связан с $d(x)$ соотношением:

$$\tilde{d}(x) = c \cdot d(x)$$

   где $c \in F$, $c \neq 0$.

   Аналогичное утверждение справедливо и в отношении НОК

   Говорят, что многочлены $f(x)$ и $g(x) \in F[x]$ ассоциированы, если $f(x) = c\, g(x)$, где $0 \neq c \in F$

Пусть сначала $m = 2$.

<u>Теорема 6</u> (алгоритм Евклида отыскания НОД многочленов $f(x)$ и $g(x)$)

Пусть $f(x), g(x) \in F[x]$, $g(x) \neq 0$

Если $f(x)$ делится на $g(x)$, то $g(x) = \text{НОД}(f(x), g(x))$ иначе

$$f(x) = g(x)\,q_1(x) + r_1(x), \quad \deg r_1(x) < \deg g(x)$$
$$g(x) = r_1(x)\,q_2(x) + r_2(x), \quad \deg r_2(x) < \deg r_1(x)$$

Метод наименьших квадратов и сингулярное разложение

Н. Н. Осипов
e-mail: nnosipov@rambler.ru

Аннотация

Статья представляет собой более подробную версию открытой лекции, прочитанной автором в мае 2016 года студентам-первокурсникам специальности «Компьютерная безопасность».

I. Рассмотрим, вообще говоря, *переопределённую* систему линейных уравнений:

$$\sum_{j=1}^{n} a_{ij}x_j = b_i, \quad i = 1, \ldots, m, \tag{0.1}$$

где $m \geqslant n$. Эту СЛУ можно записать в виде уравнения

$$\mathcal{A}(x) = b, \tag{0.2}$$

где $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$, $b = (b_1, \ldots, b_m) \in \mathbb{R}^m$ и

$$\mathcal{A} : \mathbb{R}^n \to \mathbb{R}^m$$

— *линейное отображение*, заданное матрицей $A = (a_{ij}) \in M_{m\times n}(\mathbb{R})$ в стандартных базисах арифметических векторных пространств $\mathbb{R}^n$ и $\mathbb{R}^m$.[1)] Пусть

$$a_j = \mathcal{A}(e_j) \in \mathbb{R}^m, \quad j = 1, \ldots, n,$$

— векторы, столбцы координат которых совпадают со столбцами матрицы A. Тогда уравнение (0.2) примет вид

$$x_1a_1 + \ldots + x_na_n = b.$$

Для простоты далее будем считать, что отображение $\mathcal{A}$ невырождено:

$$\operatorname{Ker}\mathcal{A} = \{0\} \tag{0.3}$$

или, в других терминах, матрица A имеет полный ранг (система векторов $(a_1, \ldots, a_n)$ линейно независима). При $m > n$ (и, тем более, при $m \gg n$, как часто бывает на практике) уравнение (0.2) обычно неразрешимо, ибо почти всегда вектор b не принадлежит подпространству

$$L = \operatorname{Im}\mathcal{A} = \langle a_1, \ldots, a_n\rangle.$$

Задача состоит в том, чтобы найти некоторое *псевдорешение*

$$x^0 = (x^0_1, \ldots, x^0_n) \in \mathbb{R}^n$$

[1)]Напомним, что стандартным базисом арифметического n-мерного векторного пространства $\mathbb{R}^n$ называется базис $(e_1, \ldots, e_n)$ из так называемых *единичных векторов* (все компоненты вектора e_j равны нулю, кроме j-й, которая равна 1).

уравнения (0.2) и тем самым как-то «решить» несовместную СЛУ (0.1).

Будем считать пространства $\mathbb{R}^n$ и $\mathbb{R}^m$ евклидовыми.[2)] В *методе наименьших квадратов* псевдорешение $x^0 \in \mathbb{R}^n$ находят, исходя из следующего условия:

$$\min_{x\in\mathbb{R}^n} |b - \mathcal{A}(x)|^2 = |b - \mathcal{A}(x^0)|^2.$$

Это условие объясняет название самого метода, так как величина $|b-\mathcal{A}(x)|^2$, которую требуется минимизировать, есть сумма квадратов

$$\sum_{i=1}^{m}\left(b_i - \sum_{j=1}^{n} a_{ij}x_j\right)^2 .$$

Метод наименьших квадратов широко применяется как в прикладной математике, так и в статистике.[3)]

Имеем $b = b' + b''$, где $b' \in L$ — *ортогональная проекция* вектора b на подпространство L, а $b'' \in L^\perp$. Пусть $a = \mathcal{A}(x) = x_1a_1 + \ldots + x_na_n \in L$. Тогда по *теореме Пифагора*

$$|b-\mathcal{A}(x)|^2 = |b-a|^2 = |(b-b') + (b'-a)| = |b-b'|^2 + |b'-a|^2 \geqslant |b-b'|^2,$$

причём равенство возможно только если $a = b'$. Итак, псевдорешение x^0 должно удовлетворять уравнению

$$x_1a_1 + \ldots + x_na_n = b'. \tag{0.4}$$

Из условия (0.3) следует, что это уравнение разрешимо и имеет единственное решение.

Стандартный теоретический способ решить уравнение (0.4) состоит в том, чтобы решить так называемую *нормальную* СЛУ

$$\sum_{j=1}^{n}(a_i, a_j)x_j = (a_i, b), \quad i = 1, \ldots, n, \tag{0.5}$$

которая получится, если для каждого $i = 1, \ldots, n$ обе части уравнения (0.4) скалярно домножить на вектор a_i и учесть, что $(a_i, b') = (a_i, b)$. Матрица системы (0.5) есть *матрица Грама*

$$G = ((a_i, a_j)) = A^tA \in M_{n\times n}(\mathbb{R})$$

системы векторов $(a_1, \ldots, a_n)$. Поскольку последняя является базисом подпространства L, имеем $\det G > 0$.[4)] Таким образом, псевдорешение x^0 можно найти по формуле

$$\begin{bmatrix} x_1^0 \\ \vdots \\ x_n^0 \end{bmatrix} = G^{-1}A^t \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} . \tag{0.6}$$

[2)]Термин «евклидово пространство $\mathbb{R}^n$» в данном случае означает, что в пространстве $\mathbb{R}^n$ задано стандартное скалярное произведение:

$$(x, y) = x_1y_1 + \ldots + x_ny_n,$$

где $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$.

[3)]Подробнее см. по ссылке [3].

[4)]Действительно, пусть $(w_1, \ldots, w_n)$ — какой-нибудь ортонормированный базис L. Тогда $G = T^tT$, где T — *матрица перехода* от $(w_1, \ldots, w_n)$ к $(a_1, \ldots, a_n)$. Следовательно, $\det G = (\det T)^2 > 0$.

II. Насколько хорош описанный выше способ отыскания псевдорешения с практической точки зрения?

Дело в том, что как матрица A, так и вектор b обычно заданы с какой-то погрешностью:

$$A \approx \hat{A}, \quad b \approx \hat{b}.$$

Возникает вопрос, насколько сильно может отличаться фактически вычисленное псевдорешение $\hat{x}^0$, соответствующее матрице $\hat{A}$ и вектору $\hat{b}$, от истинного псевдорешения x^0.[5)]

В том, что применение формулы (0.6) на практике может оказаться небезобидным, показывает уже тривиальный случай $m = n$. В этом случае

$$G^{-1}A^t = (A^tA)^{-1}A^t = A^{-1},$$

и формула (0.6) упрощается до традиционной:

$$\begin{bmatrix} x_1^0 \\ \vdots \\ x_n^0 \end{bmatrix} = A^{-1} \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}.$$

Проводить вычисления по этой формуле надёжнее, чем по формуле (0.6), поскольку лишние умножения матриц, вообще говоря, способствуют росту погрешности.

III. Опишем другой способ отыскания псевдорешения x^0, основанный на так называемом *сингулярном разложении* матрицы A, которое имеет вид

$$A = U\Sigma V^t. \tag{0.7}$$

Здесь $U \in M_{m\times m}(\mathbb{R})$, $V \in M_{n\times n}(\mathbb{R})$ — *ортогональные матрицы*, $\Sigma \in M_{m\times n}(\mathbb{R})$ — *диагональная прямоугольная матрица*.[6)]

Объясним, как можно прийти к равенству (0.7). Рассмотрим линейный оператор

$$\mathcal{G} = \mathcal{A}^*\mathcal{A} : \mathbb{R}^n \to \mathbb{R}^n,$$

заданный матрицей G в стандартном базисе. Оператор $\mathcal{G}$ является *самосопряжённым*, поскольку $G^t = G$. Следовательно, существует ортонормированный базис $(v_1, \ldots, v_n)$ пространства $\mathbb{R}^n$, состоящий из собственных векторов этого оператора:

$$\mathcal{G}(v_j) = \lambda_j v_j, \quad j = 1, \ldots, n.$$

Этот базис называется *первым сингулярным базисом* матрицы A.[7)] Кроме того, имеем

$$\lambda_j = (v_j, \mathcal{G}(v_j)) = (v_j, \mathcal{A}^*(\mathcal{A}(v_j))) = (\mathcal{A}(v_j), \mathcal{A}(v_j)) = |\mathcal{A}(v_j)|^2 > 0$$

[5)] Отметим, что и сам процесс вычисления псевдорешения $\hat{x}^0$ происходит с какой-то погрешностью (например, имеют место ошибки округления), которую также необходимо учитывать.

[6)] Напомним, что квадратная вещественная матрица C называется ортогональной, если $C^{-1} = C^t$. Подробнее о Singular Value Decomposition (SVD) и современных методах его нахождения см. по ссылке [4].

[7)] Или линейного отображения $\mathcal{A}$. Все результаты о сингулярном разложении можно излагать как на языке матриц, так и на языке линейных отображений (операторов).

для любого $j = 1, \ldots, n$. Числа

$$\sigma_j = \sqrt{\lambda_j} = |\mathcal{A}(v_j)|, \quad j = 1, \ldots, n,$$

называются *сингулярными числами* матрицы A. Далее положим

$$u_j = \frac{\mathcal{A}(v_j)}{\sigma_j}, \quad j = 1, \ldots, n.$$

Система векторов $(u_1, \ldots, u_n)$ является ортонормированным базисом подпространства L:

$$(u_i, u_j) = \frac{1}{\sigma_i \sigma_j}\,(\mathcal{A}(v_j), \mathcal{A}(v_j)) = \frac{1}{\sigma_i \sigma_j}\,(v_i, \mathcal{G}(v_j)) = \frac{\lambda_j}{\sigma_i \sigma_j}\,(v_i, v_j) = \begin{cases} 1, & \text{если } i = j, \\ 0, & \text{если } i \neq j. \end{cases}$$

Дополним её до ортонормированного базиса $(u_1, \ldots, u_m)$ всего пространства $\mathbb{R}^m$. Он называется *вторым сингулярным* базисом матрицы A.

Теперь составим ортогональные матрицы U и V из столбцов координат векторов второго и первого сингулярных базисов соответственно, а диагональную матрицу Σ заполним сингулярными числами. Тогда

$$U\Sigma = AV$$

по построению, откуда, домножив справа на $V^{-1} = V^t$, получим (0.7).

Зная сингулярное разложение (0.7) матрицы A, псевдорешение x^0 СЛУ (0.1) можно найти по формуле

$$x^0 = \sum_{j=1}^{n} \frac{(u_j, b)}{\sigma_j}\, v_j. \tag{0.8}$$

Для доказательства формулы (0.8) достаточно проверить, что она даёт решение уравнения (0.4). В самом деле, имеем

$$x_1^0 a_1 + \ldots + x_n^0 a_n = \mathcal{A}(x^0) = \sum_{j=1}^{n} \frac{(u_j, b)}{\sigma_j} \mathcal{A}(v_j) = \sum_{j=1}^{n} (u_j, b) u_j = b'.$$

IV. Вернёмся к вопросу о погрешности при вычислении псевдорешения x^0, которая может возникнуть из-за того, что матрица A и вектора b сами заданы с некоторой погрешностью.

Для простоты будем считать, что матрица A задана точно ($\hat{A} = A$), а возмущению подвергается только вектор b. Упорядочим сингулярные числа матрицы A по невозрастанию:

$$\sigma_1 \geqslant \ldots \geqslant \sigma_n > 0.$$

Пусть теперь $\hat{b} = b + \varepsilon u_n$, где коэффициент ε — малое число. Из формулы (0.8) находим

$$\hat{x}^0 = x^0 + \frac{\varepsilon}{\sigma_n}\, v_n$$

при этом коэффициент ε/σ_n может оказаться существенным, если сингулярное число σ_n мало, а коэффициент ε соизмерим с σ_n. Таким образом, при практическом вычислении следует учитывать, что псевдорешение x^0 будет особенно чувствительно к возмущениям вектора b вдоль тех векторов второго сингулярного базиса матрицы A, которые соответствуют малым сингулярным числам.

Впрочем, практический интерес представляет оценка не абсолютной, а относительной погрешности вычисления x^0, а именно, сравнение последней с той относительной погрешностью, с которой задан вектор b. Пусть

$$\Delta = \frac{|\hat{x}^0 - x^0|}{|x^0|}, \quad \delta = \frac{|\hat{b} - b|}{|b|}.$$

С помощью формулы (0.8) нетрудно получить оценку

$$\frac{\Delta}{\delta} \leqslant \frac{|b|}{|b'|} \cdot \frac{|u'|}{|u|} \cdot \frac{\sigma_1}{\sigma_n},$$

где $u = \hat{b} - b = u' + u''$ ($u' \in L$, $u'' \in L^{\perp}$). При $b \in L$ и $u \in L$ эта оценка упрощается до

$$\frac{\Delta}{\delta} \leqslant \frac{\sigma_1}{\sigma_n}.$$

Отношение σ_1/σ_n называется *числом обусловленности* матрицы A и обозначается $\mu(A)$.[8] Ясно, что чем больше $\mu(A)$, тем более неустойчивым будет вычисление псевдорешения x^0.

Отметим, что сингулярное разложение матрицы G можно получить из сингулярного разложения (0.7) матрицы A. Оно имеет вид

$$G = V\Lambda V^t,$$

при этом на диагонали матрицы

$$\Lambda = \Sigma^t\Sigma \in M_{n\times n}(\mathbb{R})$$

находятся собственные числа $\lambda_j = \sigma_j^2$ матрицы G. Поэтому $\mu(G) = \mu(A)^2 \gg \mu(A)$, если $\mu(A)$ велико. Это значит, что в этом случае вычисление псевдорешения x^0 по формуле (0.6) будет гораздо более неустойчивым, чем по формуле (0.8).

Замечание. 1. Подробное изложение различных практических способов поиска псевдорешений читатель может найти, например, в учебнике [1], глава IV. Там же (см. § 4 главы IV) можно узнать о применении метода наименьших квадратов в статистике (*линейная регрессия*).

2. При $m = n$ из сингулярного разложения (0.7) матрицы A можно получить её *полярное разложение* (см. учебник [1], §§ 1 — 3 главы I) в виде

$$A = SR, \tag{0.9}$$

где $S = U\Sigma U^t$, $R = UV^t$. Последние формулы также показывают, как от полярного разложения (0.9) матрицы A прийти к её сингулярному разложению.[9]

[8] Число $\mu(A)$ естественным образом возникает при оценке относительной погрешности решения невырожденной системы линейных уравнений (см., например, [2], стр. 14).

[9] Такая тесная связь между полярным и сингулярным разложениями матрицы неудивительна, поскольку конструкция обоих разложений основана на сингулярных базисах.

Список литературы

[1] *Беклемишев Д.В.* Дополнительные главы линейной алгебры. М.: Наука, 1983.

[2] *Годунов С.К.* Решение систем линейных уравнений. Новосибирск: Наука, 1980.

[3] https://en.wikipedia.org/wiki/Linear_least_squares_(mathematics)

[4] https://en.wikipedia.org/wiki/Singular_value_decomposition

1.6 3. Неприводимые многочлены над полем. Теорема о факторизации.

Аналогично определяется наименьшее общее кратное (НОК) ненулевых многочленов $f_1(x), \dots, f_m(x)$: слово „делитель" заменяется на „кратное".

Равенство вида

$$d(x) = \text{НОД}\,(f_1(x), \dots, f_m(x))$$

означает, что многочлен $d(x)$ является одним из НОД многочленов $f_1(x), \dots, f_m(x)$.

Аналогично следует понимать равенство

$$m(x) = \text{НОК}\,(f_1(x), \dots, f_m(x))$$

Замечание

1. Из определений формально не следует, что НОД и НОК данных многочленов существуют.

   На самом деле, как будет показано ниже, они существуют.

2. Если $d(x)$ некоторый НОД многочленов $f_1(x), \dots, f_m(x)$, то любой другой НОД этих многочленов $\tilde{d}(x)$ связан с $d(x)$ соотношением:

   $$\tilde{d}(x) = c \cdot d(x)$$

   где $c \in F$, $c \neq 0$.

   Аналогичное утверждение справедливо и в отношении НОК

   Говорят, что многочлены $f(x)$ и $g(x) \in F[x]$ ассоциированы, если $f(x) = c\, g(x)$, где $0 \neq c \in F$

Пусть сначала $m = 2$.

Теорема 6 (алгоритм Евклида отыскания НОД многочленов $f(x)$ и $g(x)$)

Пусть $f(x), g(x) \in F[x]$, $g(x) \neq 0$

Если $f(x)$ делится на $g(x)$, то $g(x) = \text{НОД}(f(x), g(x))$ иначе

$$f(x) = g(x)\, q_1(x) + r_1(x), \quad \deg r_1(x) < \deg g(x)$$
$$g(x) = r_1(x)\, q_2(x) + r_2(x), \quad \deg r_2(x) < \deg r_1(x)$$

$$r_1(x) = r_2(x)q_3(x) + r_3(x) \quad \deg r_3(x) < \deg r_2(x)$$

$\ldots$

$$r_{n-2}(x) = r_{n-1}(x)q_n(x) + r_n(x) \quad \deg r_n(x) < \deg r_{n-1}(x)$$

$$r_{n-1}(x) = r_n(x)q_{n+1}(x)$$

для некоторого $n \geq 1$.

Тогда $r_n(x) = \text{НОД}(f(x), g(x))$

Эта процедура последовательных делений с остатком наз. алгоритмом Евклида

ДОКАЗАТЕЛЬСТВО

Т.к. $\deg g(x) > \deg r_1(x) > \deg r_2(x) > \ldots$ то алгоритм Евклида конечен – завершится не более чем за $\deg g(x)$ шагов.

Если $f(x)$ делится на $g(x)$, то $g(x)$ явл. НОД $(f(x), g(x))$, т.к. соответствует определению.

Нужно теперь проверить, что $r_n(x)$ обладает всеми свойствами НОД.

Достаточно пройти по строчкам алгоритма Евклида сначала снизу вверх, а затем сверху вниз

Теорема 7 (о линейной форме НОД $(f(x), g(x))$)

Пусть $d(x) = \text{НОД}(f(x), g(x))$, где $f(x), g(x) \in F[x]$

Тогда существует $u(x), v(x) \in F[x]$ такие, что

$$d(x) = f(x)u(x) + g(x)v(x). \quad (**)$$

Можно считать, что

$$\left.\begin{aligned} \deg u(x) &< \deg g(x) - \deg d(x) \\ \deg v(x) &< \deg f(x) - \deg d(x) \end{aligned}\right\} (*)$$

ЗАМЕЧАНИЕ

Ограничения (*) дают возможность искать линейную форму НОД методом неопределенных коэффициентов.

Доказательство

Возможность линейно выразить $d(x)$ через $f(x)$ и $g(x)$ вытекает непосредственно из алгоритма Евклида

Двигаемся по строчкам алгоритма Евклида снизу вверх

Итак, можно считать, что рав-во (**) с некоторыми $u(x)$ и $v(x)$ получено.

1 Пусть сначала $d(x) = 1$. Если, например,
$$\deg u(x) < \deg g(x)$$
то обязательно
$$\deg v(x) < \deg f(x)$$
что следует из анализа равенства
$$g(x)v(x) = 1 - f(x)u(x)$$
Если же, например,
$$\deg u(x) \geq \deg g(x)$$
то разделим $u(x)$ на $g(x)$ с остатком,
$$u(x) = g(x)\cdot q(x) + \tilde{u}(x)$$
где $\deg \tilde{u}(x) < \deg g(x)$.

Имеем:
$$1 = f(x)(g(x)q(x) + \tilde{u}(x)) + g(x)v(x) =$$
$$= f(x)\tilde{u}(x) + g(x)\tilde{v}(x)$$
где $\tilde{v}(x) = v(x) + f(x)q(x)$

Причем в этом представлении уже выполнено нужное ограничение
$$\deg \tilde{u}(x) < \deg g(x)$$

2. Общий случай.

Положим $f_1(x) = f(x)/d(x)$, $g_1(x) = g(x)/d(x)$ при этом НОД $(f_1(x), g_1(x)) = 1$.

По доказанному существуют такие $u'(x)$ и $v'(x)$, что

$$1 = f_1(x)u(x) + g(x)v(x) \quad (*)$$

$$\deg u(x) < \deg g_1(x) = \deg g(x) - \deg d(x)$$

$$\deg v(x) < \deg f_1(x) = \deg f(x) - \deg d(x)$$

Ясно, что равенство $(*)$ эквивалентно (после умножения на $d(x)$) некоторому искомому линейному представлению $d(x)$

Опр. Многочлены $f_1(x), \ldots, f_m(x) \in F[x]$ называются взаимно простыми, если

$$НОД(f_1(x), \ldots, f_m(x)) = 1$$

Замечание

Из теоремы 7 вытекает следующий критерий взаимной простоты 2 многочленов:

Многочлены $f(x), g(x)$ взаимно просты $\Leftrightarrow$ существуют такие многочлены $u(x)$ и $v(x)$, что

$$1 = f(x)u(x) + g(x)v(x)$$

Свойства взаимно простых многочленов

Пусть $f(x), g(x), h(x) \in F[x]$

1. Если $f(x)g(x)$ делится на $h(x)$ и $НОД(f(x), h(x)) = 1$, то $g(x)$ делится на $h(x)$.
2. Пусть $НОД(f(x), g(x)) = 1$. Тогда $h(x)$ делится на $f(x)g(x) \Leftrightarrow h(x)$ делится и на $f(x)$, и на $g(x)$.
3. Пусть $НОД(f(x), g(x)) = НОД(f(x), h(x)) = 1$. Тогда $НОД(f(x), g(x)h(x)) = 1$.

Доказательство (1)

Имеем по критерию взаимной простоты

$$1 = f(x)u(x) + h(x)v(x)$$

для нек-рых $u(x), v(x) \in F[x]$.

Умножим обе части на $g(x)$:

$$g(x) = \underbrace{(f(x)g(x))u(x)}_{\text{делится на } h(x)} + \underbrace{h(x)}_{\text{также очевидно делится}}v(x)g(x) \Rightarrow \text{вся сумма, т.е. } g(x) \text{ делится на } h(x)$$

§14 Линейные отображения и операторы

п. 1 Линейные отображения

Опр Пусть V и W — векторные пр-ва над полем F

Отображение $\varphi: V \to W$ называется линейным, если оно обладает св-вами линейности: аддитивностью и однородностью

$$\varphi(x+y) = \varphi(x) + \varphi(y) \qquad \forall\, x, y \in V,\ k \in F$$
$$\varphi(kx) = k\varphi(x)$$

Пример

1 $V = W = \mathbb{R}^2 \quad \varphi: \mathbb{R}^2 \to \mathbb{R}^2 \quad \varphi((x_1, x_2)) = (-2x_1 + x_2, -x_1)$

Это отображение линейно: если $x = (x_1, x_2)$, $y = (y_1, y_2)$, то:

$$x + y = ((x_1 + y_1,\ x_2 + y_2))$$
$$\varphi(x) = (-2x_1 + x_2,\ -x_1)$$
$$\varphi(y) = (-2y_1 + y_2,\ -y_1)$$
$$\varphi(x+y) = (-2x - 2y_1 + x_2 - y_2,\ -x_2 - y_1) = \varphi(x) + \varphi(y)$$

Аналогично, $\varphi(kx) = k\varphi(x)$

2. $V = W = \mathbb{R}^2 \quad \varphi: \mathbb{R}^2 \to \mathbb{R}^2 \quad \varphi((x_1, x_2)) = (x_1^2, x_2^2)$

Отображение φ не является линейным

3 $V = W = \mathbb{R}^2 \quad \varphi\ \mathbb{R}^2 \to \mathbb{R} \quad \varphi(x)$ — вектор, полученный из x поворотом на $90°$

Можно показать, что это отображение линейно

Линейными будут также преобразования симметрии относительно прямой, проходящей ч/з начало координат, преобразование центральной симметрии, где центр симметрии — начало координат, преобразование поворота на угол α вокруг начала координат

4. $V = \mathbb{R}^2$, $W = \mathbb{R}^3$, $\varphi : \mathbb{R}^2 \to \mathbb{R}^3$

$$\varphi((x_1, x_2)) = (x_1 + x_2,\ x_1 - x_2,\ 0)$$

φ является линейным отображением

5. $V = \mathbb{R}^3$, $W = \mathbb{R}^2$, $\varphi : \mathbb{R}^3 \to \mathbb{R}^2$

$\varphi((x_1, x_2, x_3)) = (x_1, x_2)$ – еще один пример линейного отображения

<u>Q</u>: Как можно задавать линейные отображения?

<u>A</u>. Выберем в пр-вах V и W по базису.

$a_1, \ldots, a_n$ – базис V $\qquad n = \dim V$

$b_1, \ldots, b_m$ – базис W $\qquad m = \dim W$

а также зададим произвольную матрицу $A \in M_{m \times n}(F)$

Определим отображение $\varphi : V \to W$ следующим образом если

$$x = x_1 a_1 + \ldots + x_n a_n$$

то

$$\varphi(x) = y_1 b_1 + \ldots + y_m b_m = y$$

где

$$\begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \quad (*)$$

Не трудно проверить св-ва линейности (аддитивность и однородность) этого отображения

Эта конструкция линейного отображения является общей, т.е. любое отображение из V в W может быть так получено

Действительно, пусть $\psi (V \to W$ – произвольное такое отображение. Фиксируем произвольные базисы $a_1, \ldots, a_n$ и $b_1, \ldots, b_m$ пр-в V и W

Определим матрицу A следующим образом ее столбцы – это столбцы координат образов базисных векторов $\psi(a_j)$ $(j = 1, \ldots, n)$ в базисе $b_1, \ldots, b_m$ пр-ва W

Легко видеть, что исходное отображение ψ действует по формуле $(*)$: $\psi(x) = \psi(x_1 a_1 + \ldots + x_n a_n) = x_1 \psi(a_1) + \ldots + x_n \psi(a_n) =$
$= x_1 (a_{11} b_1 + \ldots + a_{m1} b_m) + \ldots + x_n (a_{1n} b_1 + \ldots + a_{mn} b_m) = (x_1 a_{11} + \ldots + x_n a_{1n}) b_1 + \ldots = y_1 b_1 + \ldots + y_m b_m$

Опр Так построенная матрица A называется матрицей линейного отображения $\varphi: V \to W$ в выбранных базисах

Опр. В случае $W = V$ линейное отображение называется линейным оператором, заданным на V (или линейным преобразованием пр-ва V)

Итак, всякое линейное отображение может быть задано при помощи пары базисов и матрицы. Если линейное отображение — линейный оператор, то второй базис считаем совпадающим с первым и в таком случае говорим о матрице линейного оператора в данном базисе

Пусть $\varphi: V \to W$ линейное отображение

Q: Как связаны матрицы этого отображения в различных парах базисов пр-в V и W?

A: Пусть $a_1, \dots, a_n$ и $a_1', \dots, a_n'$ — два базиса пр-ва V ($n = \dim V$), $b_1, \dots, b_m$ и $b_1', \dots, b_m'$ — два базиса пр-ва W ($m = \dim W$)

Обозначим ч/з A и A' матрицы линейного отображения φ в указанных парах базисов

Пусть также C и D — матрицы перехода от $a_1, \dots, a_n$ к $a_1', \dots, a_n'$ и от $b_1, \dots, b_m$ к $b_1', \dots, b_m'$ соответственно.

Имеем:

$$(a_1' \dots a_n') = (a_1 \dots a_n) \cdot C$$

$$(b_1' \dots b_m') = (b_1 \dots b_m) \cdot D$$

$$(\varphi(a_1) \dots \varphi(a_n)) = (b_1 \dots b_m) A$$

$$(\varphi(a_1') \dots \varphi(a_n')) = (b_1' \dots b_m') A'$$

След-но,

$$(\varphi(a_1') \dots \varphi(a_n')) = (\varphi(a_1) \dots \varphi(a_n)) \cdot C$$

Таким образом,

$$(b_1' \dots b_m') A' = (b_1 \dots b_m) A \cdot C$$

или

$$(b_1 \dots b_m) D A' = (b_1 \dots b_m) A C$$

1.7 4. Многочлены над C и R. Основная теорема алгебры многочленов и её следствия. Многочлены над Q. Критерий Эйзенштейна неприводимости многочлена над Q.

$$1 = f_1(x)u(x) + g(x)v(x) \quad (*)$$

$$\deg u(x) < \deg g_1(x) = \deg g(x) - \deg d(x)$$

$$\deg v(x) < \deg f_1(x) = \deg f(x) - \deg d(x)$$

Ясно, что равенство $(*)$ эквивалентно (после умножения на $d(x)$) некоторому искомому линейному представлению $d(x)$

Опр Многочлены $f_1(x), \ldots, f_m(x) \in F[x]$ называются взаимно простыми, если

$$НОД(f_1(x), \ldots, f_m(x)) = 1$$

Замечание

Из теоремы 7 вытекает следующий критерий взаимной простоты 2 многочленов:

Многочлены $f(x), g(x)$ взаимно просты $\Leftrightarrow$ существуют такие многочлены $u(x)$ и $v(x)$, что

$$1 = f(x)u(x) + g(x)v(x)$$

Свойства взаимно простых многочленов

Пусть $f(x), g(x), h(x) \in F[x]$

1. Если $f(x)g(x)$ делится на $h(x)$ и $НОД(f(x), h(x)) = 1$, то $g(x)$ делится на $h(x)$.

2. Пусть $НОД(f(x), g(x)) = 1$. Тогда $h(x)$ делится на $f(x)g(x) \Leftrightarrow h(x)$ делится и на $f(x)$, и на $g(x)$.

3. Пусть $НОД(f(x), g(x)) = НОД(f(x), h(x)) = 1$. Тогда $НОД(f(x), g(x)h(x)) = 1$.

Доказательство (1)

Имеем по критерию взаимной простоты

$$1 = f(x)u(x) + h(x)v(x)$$

для нек-рых $u(x), v(x) \in F[x]$.

Умножим обе части на $g(x)$ -

$$g(x) = \underbrace{(f(x)g(x))u(x)}_{\text{делится на } h(x)} + h(x)v(x)g(x)$$

также очевидно делится $\Rightarrow$ вся сумма, т.е. $g(x)$ делится на $h(x)$

Опр Так построенная матрица A называется матрицей линейного отображения $\varphi: V \to W$ в выбранных базисах

Опр. В случае $W = V$ линейное отображение называется линейным оператором, заданным на V (или линейным преобразованием пр-ва V)

И так, всякое линейное отображение может быть задано при помощи пары базисов и матрицы. Если линейное отображение — линейный оператор, то второй базис считаем совпадающим с первым и в таком случае говорим о матрице линейного оператора в данном базисе

Пусть $\varphi: V \to W$ линейное отображение

Q: Как связаны матрицы этого отображения в различных парах базисов пр-в V и W?

A: Пусть $a_1, \dots, a_n$ и $a_1', \dots, a_n'$ — два базиса пр-ва V ($n = \dim V$), $b_1, \dots, b_m$ и $b_1', \dots, b_m'$ — два базиса пр-ва W ($m = \dim W$)

Обозначим ч/з A и A' матрицы линейного отображения φ в указанных парах базисов

Пусть также C и D — матрицы перехода от $a_1, \dots, a_n$ к $a_1', \dots, a_n'$ и от $b_1, \dots, b_m$ к $b_1', \dots, b_m'$ соответственно.

Имеем:

$$(a_1' \dots a_n') = (a_1 \dots a_n) \cdot C$$

$$(b_1' \dots b_m') = (b_1 \dots b_m) \cdot D$$

$$(\varphi(a_1) \dots \varphi(a_n)) = (b_1 \dots b_m) A$$

$$(\varphi(a_1') \dots \varphi(a_n')) = (b_1' \dots b_m') A'$$

След-но,

$$(\varphi(a_1') \dots \varphi(a_n')) = (\varphi(a_1) \dots \varphi(a_n)) \cdot C$$

Таким образом,

$$(b_1' \dots b_m') A' = (b_1 \dots b_m) A \cdot C$$

или

$$(b_1 \dots b_m) DA' = (b_1 \dots b_m) AC$$

Поскольку $b_1, \dots, b_m$ — базис, то

$$DA' = AC$$

Отсюда

$$A' = D^{-1}AC$$

В частности, если φ — линейный оператор, то

$$A' = C^{-1}AC$$

где C — матрица перехода от одного базиса к другому.

п. 2 Ядро и образ

Пусть $\varphi: V \to W$ — линейное отображение

Опр. Образом линейного отображения φ называется его образ как отображения мн-ва V в мн-во W

$$\operatorname{Im}\varphi = \{\varphi(x) \in W \mid x \in V\} \subset W$$

Опр. Ядром линейного отображения φ называется мн-во

$$\operatorname{Ker}\varphi = \{x \in V \mid \varphi(x) = 0\} \subset V$$

Теорема 1

Если $\varphi: V \to W$ — линейное отображение, то $\operatorname{Im}\varphi$ — подпр-во W, $\operatorname{Ker}\varphi$ — подпр-во V.

Доказательство

1. Пусть $y, y' \in \operatorname{Im}\varphi$, $k \in F$

Докажем, что $y + y' \in \operatorname{Im}\varphi$, $ky \in \operatorname{Im}\varphi$

По определению $\operatorname{Im}\varphi$ имеем $y = \varphi(x)$, $y' = \varphi(x')$ для нек-рых $x, x' \in V$

След-но

$$y + y' = \varphi(x) + \varphi(x') = \varphi(x + x') \in \operatorname{Im}\varphi$$
$$ky = k\varphi(x) = \varphi(kx) \in \operatorname{Im}\varphi$$

Итак, $\operatorname{Im}\varphi$ замкнут относительно векторных операций. Поэтому $\operatorname{Im}\varphi$ — подпр-во пр-ва W (см. хар. признак под-пр-ва)

1.8 5. Векторное пространство над полем скаляров. Подпространство, характеристический признак подпространства.

Доказательство

1. Существование

Неполное частное $q(x)$ и остаток $r(x)$ находятся при помощи процедуры „деления уголом".

Продемонстрируем это на примере. Пусть

$$f(x) = 4x^3 - 2x^2 + x - 1$$

$$g(x) = x^2 - x + 1$$

(здесь $F = \mathbb{R}$)

$$\begin{array}{r|l} 4x^3 - 2x^2 + x - 1 & x^2 - x + 1 \\ \cline{2-2} -\underline{4x^3 - 4x^2 + 4x} & 4x + 2 \quad = q(x) \\ 2x^2 - 3x - 1 & \\ -\underline{2x^2 - 2x + 2} & \\ x - 3 \quad = r(x) & \end{array}$$

2. Единственность

Пусть $f(x) = g(x)\,q_1(x) + r_1(x) = g(x)\,q_2(x) + r_2(x)$ – два способа поделить $f(x)$ на $g(x)$ с остатком.

Имеем:

$$g(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x)$$

Если допустить, что $q_1(x) \neq q_2(x)$, то $r_2(x) - r_1(x) \neq 0$ и $\deg(r_2(x) - r_1(x)) < \deg g(x)$,

$$\deg(g(x)(q_1(x) - q_2(x)) \geq \deg g(x) > \deg(r_1(x) - r_2(x))$$

противоречие, след-но $q_1(x) = q_2(x)$ и $r_1(x) = r_2(x)$.

Опр. Пусть $f_1(x), \ldots, f_m(x) \in F[x]$ – многочлены, среди к-рых есть отличные от 0

Наибольшим общим делителем (НОД) этих многочленов называется любой многочлен $d(x) \in F[x]$, обладающий следующими свойствами:

1. $f_1(x), \ldots, f_m(x)$ делятся на $d(x)$, т.е. $d(x)$ есть общий делитель $f_1(x), \ldots, f_m(x)$.

2. Если $d_1(x)$ – любой другой общий делитель многочленов $f_1(x), \ldots, f_m(x)$, то $d(x)$ делится на $d_1(x)$.

Аналогично определяется наименьшее общее кратное (НОК). ненулевых многочленов $f_1(x), \ldots, f_m(x)$: слово „делитель" заменяется на „кратное".

Равенство вида

$$d(x) = \text{НОД}(f_1(x), \ldots, f_m(x))$$

означает, что многочлен $d(x)$ является одним из НОД многочленов $f_1(x), \ldots, f_m(x)$.

Аналогично следует понимать равенство

$$m(x) = \text{НОК}(f_1(x), \ldots, f_m(x))$$

<u>Замечание</u>

1. Из определений формально не следует, что НОД и НОК данных многочленов существуют

   На самом деле, как будет показано ниже, они существуют.

2. Если $d(x)$ некоторый НОД многочленов $f_1(x), \ldots, f_m(x)$, то любой другой НОД этих многочленов $\tilde{d}(x)$ связан с $d(x)$ соотношением:

   $$\tilde{d}(x) = c \cdot d(x)$$

   где $c \in F$, $c \neq 0$.

   Аналогичное утверждение справедливо и в отношении НОК

   Говорят, что многочлены $f(x)$ и $g(x) \in F[x]$ ассоциированы, если $f(x) = c\, g(x)$, где $0 \neq c \in F$

Пусть сначала $m = 2$.

<u>Теорема 6</u> (алгоритм Евклида отыскания НОД многочленов $f(x)$ и $g(x)$)

Пусть $f(x), g(x) \in F[x]$, $g(x) \neq 0$

Если $f(x)$ делится на $g(x)$, то $g(x) = \text{НОД}(f(x), g(x))$ иначе

$$f(x) = g(x)\, q_1(x) + r_1(x), \quad \deg r_1(x) < \deg g(x)$$
$$g(x) = r_1(x)\, q_2(x) + r_2(x), \quad \deg r_2(x) < \deg r_1(x)$$

Теорема 8

Пусть $f(x), g(x) \in F[x]$

Тогда

$$НОК\,(f(x), g(x)) = \frac{f(x)g(x)}{d(x)}$$

где $d(x) = НОД\,(f(x), g(x))$.

Доказательство

Обозначим

$$m(x) = \frac{f(x)g(x)}{d(x)} \in F[x]$$

и докажем, что $m(x)$ и есть $НОК\,(f(x), g(x))$, т.е. $m(x)$ – общее кратное этих многочленов (что очевидно) и если $M(x)$ – другое общее кратное, то $M(x)$ делится на $m(x)$.

Имеем:

$$M(x) = f(x)q_1(x) = g(x)q_2(x)$$

для нек-рых $q_1, q_2 \in F[x]$.

Разделим на $d(x)$:

$$f_1(x)\,q_1(x) = g_1(x)\,q_2(x)$$

где $f_1(x) = \frac{f(x)}{d(x)}$

$g_1(x) = \frac{f(x)}{d(x)}$

при этом $f_1(x)$ и $g_1(x)$ взаимно простые

По свойству 1 взаимно простых многочленов имеем:

$$q_2(x) = f_1(x)\,q_3(x)$$

подставив, получим после сокращения на $f_1(x)$.

$$q_1(x) = g_1(x)\,q_3(x)$$

что и так ясно.

Подставив в выражение для $M(x)$, получим

$$M(x) = g(x)\,f_1(x)\,q_3(x) = g(x)\frac{f(x)}{d(x)}\,q_3(x) =$$
$$= m(x)\,q_3(x)$$

т.е. $M(x)$ делится на $m(x)$.

Замечание (о НОД и НОК произвольного набора мн-в)

Д/отыскания НОД и НОК нескольких (≥ 3) многочленов используют следующие рекуррентные правила:

$$\text{НОД}(f_1(x), .., f_{m-1}(x), f_m(x)) =$$
$$= \text{НОД}(f_m(x), \text{НОД}(f_1(x), \dots, f_{m-1}(x)))$$
$$\text{НОК}(f_1(x), \dots, f_{m-1}(x), f_m(x)) =$$
$$= \text{НОК}(\text{НОК}(f_1(x), \dots, f_{m-1}(x)), f_m(x))$$

Кроме того для $\text{НОД}(f_1(x), \dots, f_m(x)) = d(x)$ справедливо утверждение о линейном представлении:

Существуют такие $u_1(x), .., u_m(x)$, что
$$d(x) = f_1(x)u_1(x) + .. + f_m(x)u_m(x)$$

п 4 Теорема о факторизации

Опр. Многочлен $P(x) \in F[x]$, $\deg P(x) > 0$ наз неприводимым (точнее, неприводимым над полем F), если $P(x)$ нельзя представить в виде
$$P(x) = P_1(x)\, P_2(x)$$
где $\deg P_i(x) > 0$ $(i = 1, 2)$
$P_1(x), P_2(x) \in F[x]$.

Примеры

1. $P(x) = ax + b \in F[x]$ неприводим над любым полем F $(a \neq 0)$.
2. $P(x) = x^2 + 1$ неприводим над $\mathbb{Q}$ и $\mathbb{R}$; над $\mathbb{C}$ этот многочлен приводим:
$$x^2 + 1 = (x+i)(x-i)$$

Замечание

Понятие неприводимости многочлена не явл. абсолютным, т.е. если $P(x) \in F[x]$ неприводим и $F \subset \bar{F}$, то $P(x)$ может оказаться приводимым над $\bar{F}$

Поскольку $b_1, \ldots, b_m$ – базис, то

$$DA' = AC$$

Отсюда

$$A' = D^{-1}AC$$

В частности, если φ – линейный оператор, то

$$A' = C^{-1}AC$$

где C – матрица перехода от одного базиса к другому.

п. 2 Ядро и образ

Пусть $\varphi: V \to W$ – линейное отображение

Опр. Образом линейного отображения φ называется его образ как отображения мн-ва V в мн-во W

$$\operatorname{Im}\varphi = \{\varphi(x) \in W \mid x \in V\} \subset W$$

Опр. Ядром линейного отображения φ называется мн-во

$$\operatorname{Ker}\varphi = \{x \in V \mid \varphi(x) = 0\} \subset V$$

Теорема 1

Если $\varphi: V \to W$ – линейное отображение, то $\operatorname{Im}\varphi$ – подпр-во W, $\operatorname{Ker}\varphi$ – подпр-во V.

Доказательство

1. Пусть $y, y' \in \operatorname{Im}\varphi$, $k \in F$

Покажем, что $y + y' \in \operatorname{Im}\varphi$, $ky \in \operatorname{Im}\varphi$

По определению $\operatorname{Im}\varphi$ имеем $y = \varphi(x)$, $y' = \varphi(x')$ для нек-рых $x, x' \in V$

След-но

$$y + y' = \varphi(x) + \varphi(x') = \varphi(x + x') \in \operatorname{Im}\varphi$$
$$ky = k\varphi(x) = \varphi(kx) \in \operatorname{Im}\varphi$$

Итак, $\operatorname{Im}\varphi$ замкнут относительно векторных операций. Поэтому $\operatorname{Im}\varphi$ – подпр-во пр-ва W (см. хар. признак под-пр-ва)

2. Док-во аналогично.

Пример

Пусть $\varphi: \mathbb{R}^2 \to \mathbb{R}^3$, $\varphi((x_1, x_2)) = (x_1 + x_2, x_1 - x_2, 0)$

Найдем матрицу этого линейного отображения в канонических базисах пр-в $\mathbb{R}^2$ и $\mathbb{R}^3$

$$a_1 = (1, 0), \quad a_2 = (0, 1)$$

$$b_1 = (1, 0, 0), \quad b_2 = (0, 1, 0), \quad b_3 = (0, 0, 1)$$

$$\varphi(a_1) = (1, 1, 0) = 1 \cdot b_1 + 1 b_2 + 0 \cdot b_3$$

$$\varphi(a_2) = (1, -1, 0) = 1 \cdot b_1 - 1 \cdot b_2 + 0 \cdot b_3$$

Итак, матрица линейного отображения есть

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

Если вектор x имеет в базисе a_1, a_2 координаты x_1, x_2, то вектор $y = \varphi(x)$ имеет в базисе b_1, b_2, b_3 координаты y_1, y_2, y_3, где

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = A \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

Найдем $\operatorname{Ker} \varphi$. Для этого необходимо решить систему линейных ур-ий:

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\begin{cases} x_1 + x_2 = 0, \\ x_1 - x_2 = 0; \end{cases} \Longleftrightarrow \begin{cases} x_1 = 0, \\ x_2 = 0, \end{cases}$$

Итак, $\operatorname{Ker} \varphi = \{0\}$.

Найдем $\operatorname{Im} \varphi$. Для этого заметим, что

$$\operatorname{Im} \varphi = \langle \varphi(a_1), \varphi(a_2) \rangle$$

Это общий факт, справедливый для произвольного отображения линейного $\varphi: V \to W$, т.е.

$$\operatorname{Im} \varphi = \langle \varphi(a_1), \dots, \varphi(a_n) \rangle$$

где $a_1, \dots, a_n$ – базис V.

Так как

$\varphi(a_1) = (1, 1, 0)$

$\varphi(a_2) = (1, -1, 0)$

то $\varphi(a_1), \varphi(a_2)$ — базис $\operatorname{Im}\varphi$

Таким образом,

$\dim \operatorname{Ker}\varphi = 0$

$\dim \operatorname{Im}\varphi = 2$

Теорема 2

Пусть $\varphi: V \to W$ — линейное отображение.

Тогда

$$\dim \operatorname{Ker}\varphi + \dim \operatorname{Im}\varphi = \dim V$$

Доказательство

Выберем $a_1, \dots, a_k$ подпр-ва $\operatorname{Ker}\varphi$ ($k = \dim \operatorname{Ker}\varphi$)

Дополним линейно независимую систему $a_1, \dots, a_k$ до базиса $a_1, \dots, a_k, a_{k+1}, \dots, a_n$ всего пр-ва V ($n = \dim V$).

Покажем, что векторы $\varphi(a_{k+1}), \dots, \varphi(a_n)$ образуют базис $\operatorname{Im}\varphi$

1. Векторы $\varphi(a_{k+1}), \dots, \varphi(a_n)$ линейно независимы

Пусть

$$l_1 \varphi(a_{k+1}) + \dots + l_{n-k} \varphi(a_n) = 0$$

Значит,

$$\varphi(l_1 a_{k+1} + \dots + l_{n-k} a_n) = 0$$

След-но,

$$l_1 a_{k+1} + \dots + l_{n-k} a_n \in \operatorname{Ker}\varphi$$

Так как базис $\operatorname{Ker}\varphi$ составляют $a_1, \dots, a_k$, то должно быть

$$l_1 = \dots = l_{n-k} = 0$$

2. Всякий вектор $y \in \mathrm{Im}\,\varphi$ является нек-рой линейной комбинацией $\varphi(a_{k+1}), \dots, \varphi(a_n)$

Имеем:

$$y = \varphi(x)$$

для нек-рого $x \in V$.

Разложим x по базису $a_1, \dots, a_n$:

$$x = \underbrace{l_1 a_1 + \dots + l_k a_k}_{\in \mathrm{Ker}\,\varphi} + l_{k+1} a_{k+1} + \dots + l_n a_n$$

Значит,

$$y = \varphi(x) = \varphi(l_{k+1} a_{k+1} + \dots + l_n a_n) =$$
$$= l_{k+1}\varphi(a_{k+1}) + \dots + l_n \varphi(a_n)$$

<u>Опр.</u> Дефектом линейного отображения называется размерность его ядра ($\dim \mathrm{Ker}\,\varphi$)

<u>Опр.</u> Рангом линейного отображения $\varphi: V \to W$ называется $\dim \mathrm{Im}\,\varphi$.

<u>Опр.</u> Линейное отображение $\varphi: V \to W$ называется невырожденным, если его дефект равен нулю, т.е. $\mathrm{Ker}\,\varphi = \{0\}$. (или его ранг равен n)

<u>Теорема 3</u> (критерий невырожденности) линейного оператора

Пусть $\varphi: V \to V$ — линейный оператор

Следующие условия эквивалентны:

1. $\mathrm{Ker}\,\varphi = \{0\}$
2. $\mathrm{Im}\,\varphi = V$, т.е φ — сюръективное отображ
3. φ — инъективное отображение
4. φ — биективное отображение

<u>Доказательство</u>

Схема док-ва: $1) \Rightarrow 2) \Rightarrow 3) \Rightarrow 4) \Rightarrow 1)$

$1) \Rightarrow 2)$

Пусть $\operatorname{Ker}\varphi = \{0\}$. Имеем:

$$\dim \operatorname{Ker}\varphi + \dim \operatorname{Im}\varphi = n$$

След-но,

$$\dim \operatorname{Im} = n - \dim \operatorname{Ker}\varphi = n = \dim V$$

Значит,

$$\operatorname{Im}\varphi = V$$

2) $\Rightarrow$ 3)

Пусть $\operatorname{Im}\varphi = V$, т.е φ сюръективно
Тогда $\operatorname{Ker}\varphi = \{0\}$

Если $x \neq y$, то $x - y \neq 0$. Поэтому

$$\varphi(x-y) \neq 0$$

т.е

$$\varphi(x) - \varphi(y) \neq 0$$

След-но,

$$\varphi(x) \neq \varphi(y)$$

3) $\Rightarrow$ 4)

Пусть φ инъективное отображение Тогда

$$\operatorname{Ker}\varphi = \{0\}$$

(если $x \neq 0$, $x \in \operatorname{Ker}\varphi$, то $\varphi(x) = 0 = \varphi(0)$ – противоречие инъективности отображения)

След-но,

$$\operatorname{Im}\varphi = V$$

т е

φ – сюръективное отображение

Таким образом, φ биективное отображение

4) $\Rightarrow$ 1)

Если φ – биективное отображение, то $\operatorname{Ker}\varphi = \{0\}$
(см предыдущее рассуждение)

1.9 9. Линейная зависимость векторов. Базис и ранг конечной системы векторов.

т. е. $M(x)$ делится на $m(x)$.

<u>Замечание</u> (о НОД и НОК произвольного набора мн-в)

Д/отыскания НОД и НОК нескольких (≥ 3) многочленов используют следующие рекуррентные правила:

$$\text{НОД}(f_1(x), .., f_{m-1}(x), f_m(x)) =$$
$$= \text{НОД}(f_m(x), \text{НОД}(f_1(x), \dots, f_{m-1}(x)))$$
$$\text{НОК}(f_1(x), \dots, f_{m-1}(x), f_m(x)) =$$
$$= \text{НОК}(\text{НОК}(f_1(x), \dots, f_{m-1}(x)), f_m(x))$$

Кроме того для $\text{НОД}(f_1(x), \dots, f_m(x)) = d(x)$ справедливо утверждение о линейном представлении:

Существуют такие $u_1(x), .., u_m(x)$, что
$$d(x) = f_1(x)u_1(x) + .. + f_m(x)u_m(x)$$

п 4 Теорема о факторизации

<u>Опр.</u> Многочлен $P(x) \in F[x]$, $\deg P(x) > 0$ наз неприводимым (точнее, неприводимым над полем F), если $P(x)$ нельзя представить в виде
$$P(x) = P_1(x)\, P_2(x)$$
где $\deg P_i(x) > 0 \quad (i = 1, 2)$
$P_1(x), P_2(x) \in F[x]$.

<u>Примеры</u>

1. $P(x) = ax + b \in F[x]$ неприводим над любым полем F $(a \neq 0)$.
2. $P(x) = x^2 + 1$ неприводим над $\mathbb{Q}$ и $\mathbb{R}$; над $\mathbb{C}$ этот многочлен приводим:
$$x^2 + 1 = (x + i)(x - i)$$

<u>Замечание</u>

Понятие неприводимости многочлена не явл. абсолютным, т. е. если $P(x) \in F[x]$ неприводим и $F \subset \tilde{F}$, то $P(x)$ может оказаться приводимым над $\tilde{F}$

Лемма (основное свойство неприводимых многочленов)

Пусть $p(x), f_1(x), \dots, f_m(x) \in F[x]$, причем $p(x)$ неприводим

Если $f_1(x) \dots f_m(x)$ делится на $p(x)$, то один из множителей $f_i(x)$ $(i = 1, \dots, m)$ делится на $p(x)$.

Доказательство

Пусть, от противного, ни один из $f_i(x)$ не делится на $p(x)$.

Тогда

$$НОД(p(x), f_i(x)) = 1$$

для всех $i = 1, \dots, m$

Но в таком случае произведение $f_1(x) \dots f_m(x)$ взаимно просто с $p(x)$ по св-ву взаимно простых многочленов. и потому не может делиться на $p(x)$ — противоречие

Теорема 9 (теорема о факторизации)

Пусть $f(x) \in F[x]$, $\deg f(x) > 0$

Тогда существует разложение

$$f(x) = p_1(x) \cdot \dots \cdot p_m(x) \quad (*)$$

где $p_i(x) \in F[x]$ $(i = 1, \dots, m)$ — неприводимый над F мн-н

Если

$$f(x) = q_1(x) \dots q_t(x)$$

другое такое разложение, то $t = m$ и, возможно после перенумерации, $p_i(x)$ ассоциирован с $q_i(x)$ $(i = 1, \dots, m)$, т.е. $q_i(x) = c_i p_i(x)$, $c_i \in F$, $c_i \neq 0$

Доказательство

Существование разложения (*) очевидно — достаточно рассмотреть самое длинное разложение многочлена $f(x)$ в произведение нескольких многочленов положительной степени, к-рое обязано состоять из неприводимых многочленов.

Единственность разложения необходимо доказывать, оно неочевидно. Рассм. пример мультипликативной системы, принадлежащий Гильберту.

$$S = \{4k+1 \mid k = 0, \ldots\}$$

S - мультипликативное мн-во, содержащее единицу (аналог натурального ряда)

Число $p \in S$ назовем простым, если невозможно представление

$$p = p_1 p_2$$

где $p_1, p_2 \in S$, $p_1 > 1$, $p_2 > 1$

Числа $5, 9, 13, 17, \ldots$ - простые. Очевидно, что любое число $a \in S$ разлагается в произведение простых

$$a = p_1 p_2 \cdots p_s$$

Но единственности разложения нет. Например,

$$441 = 49 \cdot 9 = 21 \cdot 21$$

Докажем единственность многочлена $f(x)$ в произведение неприводимых множителей.

Пусть

$$f(x) = p_1(x) p_2(x) \cdots p_s(x) = q_1(x) q_2(x) \cdots q_t(x)$$

два таких разложения. Левая часть этого рав-ва (а значит и правая) делится на $p_1(x)$. Но тогда один из многочленов $q_i(x)$ делится на $p_1(x)$.

Пусть, например, $q_1(x)$ делится на $p_1(x)$. Так как $q_1(x)$ неприводимый мн-н, то $q_1(x)$ пропорционален $p_1(x)$, т.е.

$$q_1(x) = c_1 p_1(x)$$

где $c_1 \neq 0$ - константа.

Сокращая на $p_1(x)$ получим:

$$p_2(x) \cdots p_s(x) = c_1 q_2(x) \cdots q_t(x)$$

Применяя это рассуждение нужное кол-во раз, придем к следующему:

$$1 = c_1 \cdot\ldots\cdot c_s\, q_{s+1}(x)\ldots q_t(x)$$

(считаем, что $t \geq s$).

При $t > s$ будем иметь противоречие.
Значит, $t = s$ и $q_i(x) = c_i p_i(x)$ $(i = 1, \ldots, s)$

Обычно разложение данного многочлена $f(x) \in F[x]$ на неприводимые множители записывают в виде:

$$f(x) = c \cdot p_1(x)^{k_1} \cdot\ldots\cdot p_s(x)^{k_s}$$

где $p_1(x), \ldots, p_s(x)$ попарно непропорциональные нормированные неприводимые над F мн-ны (нормированные — старший коэф. — единица)

Эта запись единственна с точностью до нумерации мн-нов $p_1(x), \ldots, p_s(x)$

Указанная запись наз. КАНОНИЧЕСКИМ РАЗЛОЖЕНИЕМ мн-на $f(x) \in F[x]$.

Если известно каноническое разложение мн-нов $f_1(x), \ldots, f_m(x) \in F[x]$, то НОД и НОК этих мн-в могут быть найдены при помощи хорошо известного школьного правила

Замечание

На практике предпочтительнее, вообще говоря, использовать для отыскания НОД и НОК алгоритм Евклида.

Опр. Пусть $f(x) \in F[x]$, $f(x) = a_n x^n + \ldots + a_1 x + a_0$

Производной этого мн-на наз. многочлен вида

$$f'(x) = n a_n x^{n-1} + \ldots + a_1 \in F[x]$$

Здесь $k a_k$ понимается как $\underbrace{a_k + \ldots + a_k}_{k \text{ слагаемых}}$

Пример

$F = F_2$ - поле из 2х эл-тов

Пусть $f(x) = x^2 + 1$. Тогда $f'(x) = (1+1)x = 0$

(*) Далее будем считать, что F — поле нулевой характеристики ($\operatorname{char} F = 0$), т.е. суммы вида $1 + 1 + \ldots + 1$ отличны от нуля. В этом случае, как легко видеть

$$\deg f'(x) = \deg f(x) - 1$$

Алгебра линейных операторов

Определим действия над линейными операторами $\varphi: V \to V$ (V – векторное пр-во над полем F)

Опр. Суммой линейных операторов $\varphi, \psi: V \to V$ называется линейный оператор $\varphi + \psi: V \to V$, заданный правилом:

$$(\varphi + \psi)(x) = \varphi(x) + \psi(x) \quad \forall x \in V$$

Опр. Произведением линейного оператора $\varphi: V \to V$ на скаляр $k \in F$ называется линейный оператор $k\varphi: V \to V$, действующий по правилу:

$$(k\varphi)(x) = k\varphi(x) \quad \forall x \in V$$

Замечание

Сумма линейных операторов и произведение линейного оператора на скаляр являются линейными операторами, что проверяется непосредственно

Свойства (φ, ψ, χ – линейные операторы $V \to V$)

1. $\varphi + (\psi + \chi) = (\varphi + \psi) + \chi$ (ассоциативность слож)
2. $\varphi + \psi = \psi + \varphi$ (коммутативность сложения)
3. $\varphi + O = \varphi$, где $O: V \to V$ - нулевой оператор
4. Для любого φ существует такой ψ, что

   $\varphi + \psi = O$

   ψ – противоположный линейный оператор, обозначаемый $-\varphi$
5. $k(\ell\varphi) = (k\ell)\varphi$ $(k, \ell \in F)$ (смешанная асс-ть)
6. $(k+\ell)\varphi = k\varphi + \ell\varphi$ $\quad k(\varphi+\psi) = k\varphi + k\psi$ $(k, \ell \in F)$

   (дистрибутивность)
7. $1 \cdot \varphi = \varphi$

Теорема 4

Мн-во всех линейных операторов $\varphi: V \to V$ относительно операций сложения и умножения на скаляр представляет собой векторное пр-во над полем F.

Доказательство

см. св-ва 1, – 7.

Опр. Произведением линейных операторов $\varphi, \psi: V \to V$ называется линейный оператор $\varphi \circ \psi: V \to V$, действующий по правилу

$$(\varphi \circ \psi)(x) = \varphi(\psi(x)) \quad \forall x \in V$$

Замечание

Так определенное произведение линейных операторов действительно будет линейным оператором:

$$(\varphi \circ \psi)(x+y) = \varphi(\psi(x+y)) = \varphi(\psi(x)+\psi(y)) =$$
$$= \varphi(\psi(x)) + \varphi(\psi(x)) = (\varphi\circ\psi)(x) + (\varphi\circ\psi)(y)$$

и аналогично для св-ва однородности

Свойства

φ, ψ, χ – линейные операторы $V \to V$

1. $\varphi \circ (\psi \circ \chi) = (\varphi \circ \psi) \circ \chi$
2. $\varphi \circ (\psi + \chi) = \varphi \circ \psi + \varphi \circ \chi$

   $(\psi \circ \chi) \circ \varphi = \psi \circ \varphi + \chi \circ \varphi$
3. $k(\varphi \circ \psi) = (k\varphi) \circ \psi = \varphi \circ (k\psi) \quad (k \in F)$

Опр. Пусть K – кольцо и F – поле. Если K является векторным пр-вом над F, причем $k(ab) = (ka)b = a(kb)$ для любых $a, b \in K$, $k \in F$.

Тогда K называется алгеброй над полем F

Опр. Размерностью алгебры K называется ее размерность как векторного пр-ва над F

Примеры

1 Алгебра линейных операторов, действующих в векторном пр-ве V

2 Алгебра матриц порядка n

3. Алгебра многочленов

Фиксируем произвольный базис $b_1, \ldots, b_n$ пр-ва V. Тогда всякий линейный оператор $\varphi: V \to V$ может быть задан матрицей $A_\varphi \in M_n(F)$, $n = \dim V$

Соответствие $\varphi \mapsto A_\varphi$ является взаимооднозначным и связано с операциями над линейными преобразованиями следующим образом:

$$A_{\varphi+\psi} = A_\varphi + A_\psi$$

$$A_{k\varphi} = k A_\varphi$$

$$A_{\varphi\psi} = A_\varphi \cdot A_\psi$$

Убедимся в справедливости последней формулы

Находим образы базисных векторов:

$$\varphi(b_i) = \sum_{j=1}^{n} a_{ji}^{\varphi} b_j \qquad \psi(b_i) = \sum_{j=1}^{n} a_{ji}^{\psi} b_j$$

здесь $A_\varphi = (a_{ij}^{\varphi})$, $A_\psi = (a_{ij}^{\psi})$

$$(\varphi \circ \psi)(b_i) = \varphi(\psi(b_i)) = \varphi\left(\sum_{j=1}^{n} a_{ji}^{\psi} b_j\right) =$$

$$= \sum_{j=1}^{n} a_{ji}^{\psi} \varphi(b_j) = \sum_{j=1}^{n} a_{ji}^{\psi} \sum_{k=1}^{n} a_{kj}^{\varphi} b_k = \sum_{k=1}^{n} \left(\sum_{j=1}^{n} a_{kj}^{\varphi} a_{ji}^{\psi}\right) b_k$$

Отсюда и следует доказываемая формула, т.к.

$$\sum_{j=1}^{n} a_{kj} a_{ji}$$

есть ki-ый эл-нт матрицы $A_\varphi \cdot A_\psi$

Опр. Линейный оператор $\varphi: V \to V$ называется обратимым, если существует такой линейный оператор ψ, что $\varphi \circ \psi = \psi \circ \varphi = \mathcal{E}$ где $\mathcal{E}$ — тождественный линейный оператор ($\mathcal{E}(x) = x \quad \forall x$)

Обозначение

$$\psi = \varphi^{-1}$$

Теорема 5

Линейный оператор $\varphi: V \to V$ обратим тогда и только тогда, когда он является невырожденным

Доказательство

$\Rightarrow$ Пусть оператор $\varphi: V \to V$ обратим.

Тогда рав-во
$$\varphi(x) = 0$$
влечет рав-во
$$x = 0$$
Действительно, $\varphi^{-1}(\varphi(x)) = x = \varphi(0) = 0$

Значит, $\operatorname{Ker} \varphi = \{0\}$, т.е φ - невырожденный оператор.

$\Leftarrow$ Пусть φ - невырожденный оператор

Тогда, во-первых, φ - инъективное отображение и, во-вторых, φ - сюръективное отображение, т.е $\varphi: V \to V$ - взаимнооднозначное отображение, поэтому определено обратное отображение $\varphi^{-1}: V \to V$, которое, как легко видеть, является линейным

Таким образом, оператор φ обратим

Замечание

Линейный оператор $\varphi: V \to V$ является невырожденным тогда и только тогда, когда $\det A_\varphi \neq 0$, где A_φ - матрица линейного оператора φ в каком-нибудь базисе:

$\dim \operatorname{Im} \varphi = \operatorname{rank} \varphi = \operatorname{rank} A_\varphi$. Если $\det A_\varphi \neq 0$, то обратный оператор $\varphi^{-1}: V \to V$ существует и $A_{\varphi^{-1}} = A_\varphi^{-1}$

1.10 10. Базис векторного пространства. Конечномерные векторные пространства.

$$1 = c_1 \cdot \ldots c_s \, q_{s+1}(x) \ldots q_t(x)$$

(считаем, что $t \geq s$).

При $t > s$ будем иметь противоречие. Значит, $t = s$ и $q_i(x) = c_i p_i(x)$ $(i = 1, \ldots, s)$

Обычно разложение данного многочлена $f(x) \in F[x]$ на неприводимые множители записывают в виде:

$$f(x) = c \cdot p_1(x)^{k_1} \cdot \ldots \; p_s(x)^{k_s}$$

где $p_1(x), \ldots, p_s(x)$ попарно непропорциональные нормированные неприводимые над F мн-ны (нормированные — старший коэф. — единица)

Эта запись единственна с точностью до нумерации мн-нов $p_1(x), \ldots, p_s(x)$

Указанная запись наз. КАНОНИЧЕСКИМ разложением мн-на $f(x) \in F[x]$.

Если известно каноническое разложение мн-нов $f_1(x), \ldots, f_m(x) \in F[x]$, то НОД и НОК этих мн-в могут быть найдены при помощи хорошо известного школьного правила

<u>Замечание</u>

На практике предпочтительнее, вообще говоря, использовать для отыскания НОД и НОК алгоритм Евклида.

<u>Опр</u> Пусть $f(x) \in F[x]$, $f(x) = a_n x^n + \ldots + a_1 x + a_0$

Производной этого мн-на наз. многочлен вида

$$f'(x) = n a_n x^{n-1} + \ldots + a_1 \in F[x]$$

Здесь $k a_k$ понимается как $\underbrace{a_k + \ldots + a_k}_{k \text{ слагаемых}}$

<u>Пример</u>

$F = F_2$ — поле из 2х эл-тов

Пусть $f(x) = x^2 + 1$. Тогда $f'(x) = (1+1)x = 0$

(*) Далее будем считать, что F — поле нулевой характеристики ($\operatorname{char} F = 0$), т.е. суммы вида $1 + 1 + \ldots + 1$ отличны от нуля. В этом случае, как легко видеть

$$\deg f'(x) = \deg f(x) - 1$$

Операция дифференцирования многочленов подчиняется обычным правилам. Например, имеет место формула Лейбница

$$\left(f(x)g(x)\right)' = f'(x)g(x) + f(x)g'(x)$$

$(f(x), g(x) \in F[x])$ Используя ее, нетрудно установить следующее утверждение: если многочлен $f(x)$ взаимно прост со своей производной $f'(x)$, то $f(x)$ не имеет кратных неприводимых делителей. (Действительно, пусть $f(x) = p(x)^k f_1(x)$, где $p(x)$ — неприводимый многочлен, $k > 1$ Тогда $f'(x) = k\,p(x)^{k-1}p'(x)f_1(x) + p(x)^k f_1'(x)$, т.е. $f'(x)$ делится по крайней мере на $p(x)^{k-1}$.) Однако обратное утверждение не всегда верно. Например, многочлен $p(x) = x^2 - t \in \in \mathbb{F}_2(t)[x]$ неприводим, но $p'(x) = 0$. Если поле F имеет нулевую характеристику, то все в порядке, так как в этом случае $\deg f'(x) = \deg f(x) - 1$.

Теорема 10

Пусть $f(x) \in F[x]$, $f(x) = p(x)^k g(x)$, где $g(x)$ не делится на $p(x)$ – неприводимый многочлен над F (т.е. $p(x)$ – неприводимый множитель мн-на $f(x)$ кратности k).

Тогда $p(x)$ – неприводимый множитель мн-на $f'(x)$ кратности $k-1$. (при $k=1$ $p(x)$ не входит в каноническое разложение $f'(x)$)

Доказательство

Справедливы правила известные дифференцирования суммы и произведения (в частности, степени)

Имеем

$$f'(x) = k\,p(x)^{k-1} p'(x) g(x) + p(x)^k g'(x) = p(x)^{k-1}\left(k p'(x) g(x) + p(x) g'(x)\right)$$

Значит, $f(x)$ делится на $p(x)^{k-1}$. Покажем, что

$$h(x) = k p'(x) g(x) + p(x) g'(x) \text{ не делится}$$

не делится на $p(x)$. Для этого достаточно установить, что

$$k p'(x) g(x)$$

не делится на $p'(x)$

Поскольку $p'(x) \neq 0$ ($\deg p'(x) = \deg p(x) - 1$), то $kp'(x) \neq 0$ ($\mathrm{char}\, F = 0$)

Если бы произведение $kp'(x)g(x)$ было кратно $p(x)$, то либо $kp'(x)$ делится на $p(x)$, что невозможно, либо $g(x)$ делится на $p(x)$, что не так по условию

Итак,

$$f'(x) = p(x)^{k-1} h(x)$$

где $h(x)$ не делится на $p(x)$

Таким образом $p(x)$ - неприводимый множитель многочлена $f'(x)$ кратности $k-1$.

Опишем процедуру выделения кратных неприводимых множителей заданного многочлена $f(x)$

Пусть

$$f(x) = cp_1(x)^{k_1} \quad p_s(x)^{k}$$

– каноническое разложение

Рассмотрим

$$d(x) = НОД\left(f(x), f'(x)\right) = \; = p_1(x)^{k_1 - 1} \quad p_s(x)^{k\ -1}$$

т е неприводимые множители $d(x)$ суть кратные неприводимые множители $f(x)$

Отыскание $d(x)$ и есть выделение в $f(x)$ кратных неприводимых множителей

Отметим, что $d(x)$ может быть найден без использования канонического разложения $f(x)$ при помощи алгоритма Евклида

Далее можно освободиться от кратных множителей, т е перейти от многочлена $f(x)$ к

$$\tilde{f}(x) = \frac{f(x)}{d(x)}$$

Имеем

$$\tilde{f}(x) = cp_1(x) \quad p_s(x),$$

т е $\tilde{f}(x)$ имеет те же неприводимые множители, что и $f(x)$, но они входят в каноническое разложение только в первой степени

Отыскав каноническое разложение $\tilde{f}(x)$, затем можно найти и каноническое разложение $f(x)$

п. 3 Собственные значения и собственные векторы

Пусть φ – линейный оператор, матрица которого в нек-ром базисе $b_1, \dots, b_n$ $(n = \dim V)$ имеет диагональный вид:

$$A_\varphi = \begin{pmatrix} \lambda_1 & \dots & 0 \\ \dots & \dots & \dots \\ 0 & \dots & \lambda_n \end{pmatrix}$$

Действие этого оператора на векторы следующее:

$$\varphi(b_1) = \lambda_1 b_1, \ \varphi(b_2) = \lambda_2 b_2, \dots, \varphi(b_n) = \lambda_n b_n$$

Если $b = k_1 b_1 + \ldots + k_n b_n \in V$, то $\varphi(b) = \lambda_1 k_1 b_1 + \ldots + \lambda_n k_n b_n$

<u>Опр.</u> Пусть $\varphi : V \to V$ – линейный оператор.

Скаляр $\lambda \in F$ называется собственным значением линейного оператора φ, если существует такой ненулевой вектор $x \in V$, что $\varphi(x) = \lambda x$

<u>Опр.</u> Вектор $x \in V$, $x \neq 0$ называется собственным вектором, принадлежащим собственному значению λ, если $\varphi(x) = \lambda x$

<u>Примеры</u>

1. Если $\varphi : V \to V$ – линейный оператор с матрицей

$$A_\varphi = \begin{pmatrix} \lambda_1 & \ldots & 0 \\ \ldots & \ldots & \ldots \\ 0 & \ldots & \lambda_n \end{pmatrix}$$

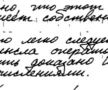
то скаляры $\lambda_1, \ldots, \lambda_n$ являются собственными значениями оператора φ

Соответственно, собственные векторы – векторы $b_1, \ldots, b_n$

Можно показать, что других собственных значений нет.

2. Рассмотрим оператор поворота на $90°$ в $\mathbb{R}^2$:

$$\varphi((x_1, x_2)) = (-x_2, x_1)$$



Ясно, что этот линейный оператор не имеет собственных значений.

Это легко следует из геометрического смысла оператора поворота, но может быть доказано и непосредственными вычислениями.

Пусть $x = (x_1, x_2)$ – собственный вектор, принадлежащий собственному значению λ, $x \neq 0$.

Тогда:

$$\varphi(x) = \lambda x \Leftrightarrow$$

$$(-x_2, x_1) = (\lambda x_1, \lambda x_2) \Leftrightarrow$$

$$\begin{cases} -x_2 = \lambda x_1 \\ x_1 = \lambda x_2 \end{cases} \Leftrightarrow \begin{cases} -\lambda x_1 - x_2 = 0 \\ x_1 - \lambda x_2 = 0 \end{cases}$$

$$\det\begin{pmatrix} -\lambda & -1 \\ 1 & -\lambda \end{pmatrix} = \lambda^2 + 1 \neq 0$$

Эта СЛУ имеет только нулевое решение, а значит собственных векторов нет ни для какого значения λ

3 Аналогично определенный линейный оператор $\varphi : \mathbb{C}^2 \to \mathbb{C}^2$ уже будет иметь собственные значения, а именно, таковыми будут корни ур-ия

$$\lambda^2 + 1 = 0$$

т.е.

$$\lambda_1 = i, \ \lambda_2 = -i$$

Матрица φ в стандартном базисе

$$e_1 = (1, 0) \quad e_2 = (0, 1)$$

имеет вид:

$$A_\varphi = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Образ $y = \varphi(x)$ имеет координаты:

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

Соотношение $\varphi(x) = \lambda x$ в координатной форме примет вид:

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \lambda x_2 \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ & \lambda \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

или

$$\begin{pmatrix} -\lambda & -1 \\ 1 & -\lambda \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

При $\lambda = i$ имеем:

$$\begin{cases} -ix_1 - x_2 = 0 \\ x_1 - ix_2 = 0 \end{cases} \Leftrightarrow -ix_1 - x_2 = 0$$

Если $x_2 = 1$, то $x_1 = i \Rightarrow$ вектор $x(i, 1)$ будет собственным вектором, принадлежащим собственному значению λ.

Пусть $\lambda = -i$. Тогда собственный вектор – вектор $b_2 = (-i, 1)$.

Видно, что b_1, b_2 – базис $\mathbb{C}^2$. Тогда данный оператор $\varphi : \mathbb{C}^2 \to \mathbb{C}^2$ можно задать более простым способом, а именно, диагональной матрицей

$$A_{\varphi'} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

в базисе из собственных векторов.

Одной из причин недиагонализируемости линейных операторов $\varphi : V \to V$ является алгебраические св-ва поля скаляров F, над к-рым задано векторное пр-во V.

Теорема 6

Пусть $\varphi : V \to V$ – линейный оператор, заданный матрицей A_φ в нек-ром базисе $b_1, \dots, b_n$ пр-ва V.

Тогда скаляр λ является собственным значением оператора $\varphi \Leftrightarrow \det(A_\varphi - \lambda E)$

Это ур-ие наз. характеристическим ур-ием оператора φ и оно не зависит от выбора матрицы линейного оператора

Если A'_φ – матрица в др. базисе, то

$$A'_\varphi = T^{-1} A_\varphi T$$

где T – матрица перехода и

$$\det(A'_\varphi - \lambda E) = \det(T^{-1} A_\varphi T - \lambda E) =$$

$$= \det(T^{-1}A_\varphi' - T^{-1}\lambda E T) =$$
$$= \det(T^{-1}(A_\varphi - \lambda E)T) =$$
$$= \det T^{-1} \det(A_\varphi - \lambda E) \det T =$$
$$= \det(A_\varphi - \lambda E).$$

Если λ – одно из собственных значений опер. φ, то принадлежащие ему собственные векторы могут быть найдены (в координатах) решения ОСЛУ

$$(A_\varphi - \lambda E)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

где $x_1, \dots, x_n$ – координаты собственного вектора в базисе $b_1, \dots, b_n$.

Доказательство

Пусть x – собственный вектор, принадлежащий собственному значению λ,

$$x = x_1 b_1 + \dots + x_n b_n$$

Это равносильно соотношению

$$\varphi(x) = \lambda x \quad (*)$$

или в координатной форме

$$A_\varphi \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix} = \lambda \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix}$$

или $(*)$ могут быть найдены как ненулевые решения ОСЛУ

$$(A_\varphi - \lambda E)\begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \dots \\ 0 \end{pmatrix}$$

Эта ОСЛУ имеет ненулевые решения $\Leftrightarrow$ $\Leftrightarrow \det(A_\varphi - \lambda E) = 0$.

Замечание

Характеристическое ур-ие линейного опер. φ имеет вид

$$\det \begin{pmatrix} a_{11}-\lambda & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22}-\lambda & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn}-\lambda \end{pmatrix}$$

или

$$(-1)^n \lambda^n + \dots = 0$$

Это алгебраическое ур-ие n-ой степени. Из теории многочленов следует, что корней этого ур-ия не более n, значит собственных значений любого линейного оператора не более $n = \dim V$.

<u>Опр.</u> Пусть $\lambda \in F$ – нек-рое собственное значение линейного оператора $\varphi: V \to V$.

Мн-во всех собственных векторов, принадлежащих собственному значению λ вместе с нулевым вектором, образует подпр-во, называемое собственным подпр-вом, соответствующим собственному значению λ.

Это подпр-во есть $\mathrm{Ker}(\varphi - \lambda \mathcal{E})$, где $\mathcal{E}$ – тождественный линейный оператор (тождественное преобразование).

<u>Обозначение</u>

$$L_\lambda = \mathrm{Ker}(\varphi - \lambda \mathcal{E})$$

собственное подпр-во оператора $\varphi: V \to V$, соотв. собственному значению λ.

<u>Опр</u> Если линейный оператор $\varphi: V \to V$ в нек-ром базисе может быть задан диагональной матрицей, то говорят, что φ – диагонализируемый линейный оператор.

Легко видеть, что любой диагонализируемый оператор имеет $n = \dim V$ линейно независимых собственных векторов.

Обратно, если линейный оператор диагонализируемый, то он имеет n линейно независимые собственные векторы.

1.11 11. Координаты вектора в базисе. Матрица перехода от одного базиса к другому. Связь между координатами вектора в разных базисах.

п 5 Поле рациональных дробей.

Опр Рациональной дробью над полем F называется класс эквивалентности выражения

вида $\dfrac{f(x)}{g(x)}$, где $f(x), g(x) \in F[x]$, $g(x) \neq 0$

Выражения $\dfrac{f(x)}{g(x)}$ и $\dfrac{f_1(x)}{g_1(x)}$ считаются эквивалентными, если

$f(x)g_1(x) = f_1(x)g(x)$

Можно показать, что это отношение является отношением эквивалентности

Обозначим через $F(x)$ множество всех рациональных дробей от x над полем F На $F(x)$ вводятся (естественным образом) операции сложения и умножения

Относительно этих операций $F(x)$ представляет собой поле рациональных дробей с коэффициентами из поля F

Замечание

Поле рациональных дробей $F(x)$ – частный случай конструкции поля отношений данного целостного кольца K

Имеем $F[x] \subset F(x)$

Опр Рациональная дробь $\dfrac{f(x)}{g(x)}$ называется правильной, если $\deg f(x) < \deg g(x)$

Любая рациональная дробь представляется (и притом единственным образом) в виде

$$q(x) + \frac{r(x)}{g(x)},$$

где $\dfrac{r(x)}{g(x)}$ – правильная рациональная дробь, $q(x)$ – многочлен (достаточно разделить $f(x)$ на $g(x)$ с остатком)

Опр Рациональная дробь вида $\dfrac{r(x)}{p(x)^k}$, где $r(x)$, $p(x)$ – многочлены, причем $p(x)$

неприводим, $\deg r(x) < \deg p(x)$, $k \in \mathbb{N}$, называется простейшей

Теорема 11

Всякая правильная рациональная дробь может быть представима (и притом единственным образом с точностью до порядка множителей) в виде суммы простейших дробей

Схема доказательства

Пусть дана правильная рациональная дробь $\dfrac{f(x)}{g(x)} \in F(x)$ Представим $g(x)$ в

каноническом виде

$$g(x) = p_1(x)^{k_1} \quad p(x)^k ,$$

где $p_i(x)$ – неприводимые над F многочлены

1 Доказываем, что $\frac{f(x)}{g(x)}$ можно представить в виде

$$\frac{f(x)}{g(x)}=\frac{f_1(x)}{p_1(x)^{k_1}}+\quad+\frac{f_s(x)}{p_s(x)^{k_s}},$$

где $f_i\in F[x]$, $\deg f_i(x)<k_i\deg p_i(x)$, т е дроби $\frac{f_i(x)}{p_i(x)^k}$ – правильные

Это представление единственно

2 Пусть имеется правильная дробь вида $\frac{\tilde{f}(x)}{p(x)^k}$, где $p\ (x)$ – неприводимый многочлен

Эту дробь можно представить, и притом единственным образом, в виде

$$\frac{\tilde{f}(x)}{p(x)^k}=\frac{r_1(x)}{p(x)}+\quad+\frac{r_k(x)}{p(x)^k}$$

где $\deg r_i(x)<\deg p(x)$

Здесь $r_k(x)$ находится как остаток от деления $\tilde{f}(x)$ на $p\ (x)$, r_{k-1} – это остаток от деления $\frac{f(x)-r_k(x)}{p(x)}$ на $p\ (x)$

Замечание

На практике разложение правильной дроби в сумму простейших обычно находят методом неопределенных коэффициентов

п. 6. Многочлены над $\mathbb{C},\mathbb{R},\mathbb{Q}$

Пусть $F=\mathbb{C}$ Следующую теорему называют основной теоремой алгебры Гаусса

Теорема 12 (теорема Гаусса)

Всякий многочлен $f(x)\in\mathbb{C}[x]$, $\deg f(x)>0$ имеет хотя бы один корень из $\mathbb{C}$

Замечание

Свойство поля $\mathbb{C}$, о котором идет речь в теореме 11, называется алгебраической замкнутостью

Доказательство

См какой-либо курс ТФКП (теория функций комплексного переменного) или стандартное доказательство, основанное на лемме Даламбера

Следствие 1

Всякий неприводимый многочлен $p(x)\in\mathbb{C}[x]$ является линейным, т е имеет вид

$$p(x)=ax+b,$$

где $a,b\in\mathbb{C}$, $a\neq 0$

Следствие 2

Всякий многочлен $f(x)\in\mathbb{C}[x]$, $\deg f(x)>0$ представляется в виде

$$a(x-x_1)^{k_1}\quad (x-x_s)^{k},$$

где $x_1,\quad ,x_s\in\mathbb{C}$ – попарно различные корни f (x) кратности $k_1\qquad k_s$ соответственно

Пусть $F=\mathbb{R}$

Лемма

Пусть $f(x)\in\mathbb{R}[x]$

Если $x_0\in\mathbb{C}$ – комплексный корень $f(x)$, то $\overline{x}_0$ – также корень $f(x)$

Доказательство

Пусть $f(x)=a_nx^n+\quad+\quad+a_1x+a_0$ Имеем

$$0=f(x_0)=a_nx_0^n+\;+\quad+a_1x+a_0$$

Тогда

$$\overline{0}=\overline{a}_n\overline{x}_0^n+\quad+\overline{a}_1\overline{x}_0+\overline{a}_0$$

Т к $a_k\in\mathbb{R}$, то $\overline{a}_k=a_k$ $(k=0,\quad ,n)$ и получаем

$$0=a_n\overline{x}_0^n+\quad+a_1\overline{x}_0+a_0,$$

т е $\overline{x}_0$ – корень $f(x)$

Следствие

Всякий неприводимый многочлен $p(x)\in\mathbb{R}[x]$ либо линеен, либо квадратичен, т е имеет вид

$$p(x)=ax^2+bx+c,$$

причем $b^2-4ac<0$

Доказательство

Пусть $p(x)$ – неприводим над $\mathbb{R}$ и $\deg p(x) > 2$ По теореме Гаусса существует $x_0 \in \mathbb{C}$ – корень $p(x)$ По лемме $\overline{x}_0$ – также корень $p(x)$ Имеем

$$p(x) = (x - x_0)(x - \overline{x}_0)q(x),$$

где $\deg q(x) > 0$

Ясно, что $q(x) \in \mathbb{R}[x]$, т к $p(x) \in \mathbb{R}[x]$ и $(x - x_0)(x - \overline{x}_0) = \; = x^2 - (x_0 + \overline{x}_0)x +$

V $+|x_0|^2 \in \mathbb{R}[x]$

Но равенство

$$p(x) = (x^2 - \; -(x_0 + \overline{x}_0)x + |x_0|^2)q(x)$$

противоречит неприводимости многочлена $p(x)$

Осталось заметить, что многочлены $ax^2 + bx + c$, $a \neq 0$, $b^2 - 4ac \geq 0$ не могут быть неприводимыми, т к имеют хотя бы один вещественный корень

Замечание

Если $f(x) \in F[x]$, $\deg f(x) = 2$ или 3, то вопрос о неприводимости $f(x)$ эквивалентен вопросу об отсутствии корней $f(x)$ в поле F

В общем случае это утверждение неверно

Пример

$$F = \mathbb{R},\; f(x) = x^4 + 4 = \; = (x^4 + 4x^2 + 4) - 4x^2 = \; = (x^2 + 2)^2 - 4x^2 = \; = (x^2 - 2x + 2)$$
$$(x^2 + 2x + 2)$$

Следствие 4

Всякий многочлен $f(x) \in \mathbb{R}[x]$, $\deg f(x) > 0$ представим в виде

$$f(x) = a(x - x_1)^{k_1} \quad (x - x_s)^{k} \; p_1(x)^{l_1} \quad p_t(x)^{l},$$

Где $x_1, \quad , x_s \in \mathbb{R}$ – попарно различные вещественные корни $f(x)$ кратности $k_1, \quad , k_s$ соответственно, $p_i(x) = x^2 + c_i x + \quad + d_i \in \mathbb{R}[x]$ – попарно различные многочлены $c_i^2 - 4d_i < 0$ $(i = 1, \quad , t)$

Пусть $F = \mathbb{Q}$ Можно доказать, что неприводимыми над $\mathbb{Q}$ могут быть многочлены любой степени Например, многочлен $p(x) = x^n - 2$, неприводим при любом $n \geq 1$ Для доказательства этого утверждения и других подобных обычно применяют признаки (достаточные условия) неприводимости Наиболее известным из них является так называемый признак Эйзенштейна

Теорема 13 (критерий Эйзенштейна)

Пусть $f(x) \in \mathbb{Z}[x]$, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \; + \quad + a_1 x + a_0$

Предположим, что существует такое простое число p что

1 a_n не делится на p

2 $a_{n-1}, \quad , a_1, a_0$ делятся на p

3 a_0 не делится на p^2

Тогда $f(x)$ неприводим над $\mathbb{Q}$

п. 3 Собственные значения и собственные векторы

Пусть φ – линейный оператор, матрица которого в нек-ром базисе $b_1, \dots, b_n$ $(n = \dim V)$ имеет диагональный вид:

$$A_\varphi = \begin{pmatrix} \lambda_1 & \dots & 0 \\ \dots & \dots & \dots \\ 0 & \dots & \lambda_n \end{pmatrix}$$

Действие этого оператора на векторы следующее:

$$\varphi(b_1) = \lambda_1 b_1, \ \varphi(b_2) = \lambda_2 b_2, \dots, \varphi(b_n) = \lambda_n b_n$$

Если $b = k_1 b_1 + \ldots + k_n b_n \in V$, то $\varphi(b) = \lambda_1 k_1 b_1 + \ldots + \lambda_n k_n b_n$

<u>Опр.</u> Пусть $\varphi : V \to V$ – линейный оператор.

Скаляр $\lambda \in F$ называется собственным значением линейного оператора φ, если существует такой ненулевой вектор $x \in V$, что $\varphi(x) = \lambda x$

<u>Опр.</u> Вектор $x \in V$, $x \neq 0$ называется собственным вектором, принадлежащим собственному значению λ, если $\varphi(x) = \lambda x$

<u>Примеры</u>

1. Если $\varphi : V \to V$ – линейный оператор с матрицей

$$A_\varphi = \begin{pmatrix} \lambda_1 & \ldots & 0 \\ \ldots & \ldots & \ldots \\ 0 & \ldots & \lambda_n \end{pmatrix}$$

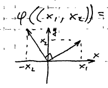
то скаляры $\lambda_1, \ldots, \lambda_n$ являются собственными значениями оператора φ

Соответственно, собственные векторы – векторы $b_1, \ldots, b_n$

Можно показать, что других собственных значений нет.

2. Рассмотрим оператор поворота на $90°$ в $\mathbb{R}^2$:

$$\varphi((x_1, x_2)) = (-x_2, x_1)$$



Ясно, что этот линейный оператор не имеет собственных значений.

Это легко следует из геометрического смысла оператора поворота, но может быть доказано и непосредственными вычислениями.

Пусть $x = (x_1, x_2)$ – собственный вектор, принадлежащий собственному значению λ, $x \neq 0$.

$$\det\begin{pmatrix} a_{11}-\lambda & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22}-\lambda & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn}-\lambda \end{pmatrix}$$

или

$$(-1)^n \lambda^n + \dots = 0$$

Это алгебраическое ур-ие n-ой степени. Из теории многочленов следует, что корней этого ур-ия не более n, значит собственных значений любого линейного оператора не более $n = \dim V$.

<u>Опр.</u> Пусть $\lambda \in F$ – нек-рое собственное значение линейного оператора $\varphi: V \to V$.

Мн-во всех собственных векторов, принадлежащих собственному значению λ вместе с нулевым вектором, образует подпр-во, называемое собственным подпр-вом, соответствующим собственному значению λ

Это подпр-во есть $\operatorname{Ker}(\varphi - \lambda\mathcal{E})$, где $\mathcal{E}$ – тождественный линейный оператор (тождественное преобразование).

<u>Обозначение</u>

$$L_\lambda = \operatorname{Ker}(\varphi - \lambda\mathcal{E})$$

собственное подпр-во оператора $\varphi: V \to V$, соотв. собственному значению λ.

<u>Опр</u> Если линейный оператор $\varphi: V \to V$ в нек-ром базисе может быть задан диагональной матрицей, то говорят, что φ – диагонализируемый линейный оператор.

Легко видеть, что любой диагонализируемый оператор имеет $n = \dim V$ линейно независимых собственных векторов.

Обратно, если линейный оператор диагонализируемый, то он имеет n линейно независимые собственные векторы.

1.12 12. Линейная оболочка системы векторов. Суммы подпространств.

Доказательство

Пусть $p(x)$ – неприводим над $\mathbb{R}$ и $\deg p(x) > 2$ По теореме Гаусса существует $x_0 \in \mathbb{C}$ – корень $p(x)$ По лемме $\overline{x}_0$ – также корень $p(x)$ Имеем

$$p(x) = (x - x_0)(x - \overline{x}_0)q(x),$$

где $\deg q(x) > 0$

Ясно, что $q(x) \in \mathbb{R}[x]$, т к $p(x) \in \mathbb{R}[x]$ и $(x - x_0)(x - \overline{x}_0) = \; = x^2 - (x_0 + \overline{x}_0)x +$

V $+|x_0|^2 \in \mathbb{R}[x]$

Но равенство

$$p(x) = (x^2 - \; -(x_0 + \overline{x}_0)x + |x_0|^2)q(x)$$

противоречит неприводимости многочлена $p(x)$

Осталось заметить, что многочлены $ax^2 + bx + c$, $a \neq 0$, $b^2 - 4ac \geq 0$ не могут быть неприводимыми, т к имеют хотя бы один вещественный корень

Замечание

Если $f(x) \in F[x]$, $\deg f(x) = 2$ или 3, то вопрос о неприводимости $f(x)$ эквивалентен вопросу об отсутствии корней $f(x)$ в поле F

В общем случае это утверждение неверно

Пример

$$F = \mathbb{R},\ f(x) = x^4 + 4 = \; = (x^4 + 4x^2 + 4) - 4x^2 = \; = (x^2 + 2)^2 - 4x^2 = \; = (x^2 - 2x + 2)$$
$$(x^2 + 2x + 2)$$

Следствие 4

Всякий многочлен $f(x) \in \mathbb{R}[x]$, $\deg f(x) > 0$ представим в виде

$$f(x) = a(x - x_1)^{k_1} \qquad (x - x_s)^{k} \; p_1(x)^{l_1} \qquad p_t(x)^{l},$$

Где $x_1, \quad , x_s \in \mathbb{R}$ – попарно различные вещественные корни $f(x)$ кратности $k_1, \quad , k_s$ соответственно, $p_i(x) = x^2 + c_i x + \quad + d_i \in \mathbb{R}[x]$ – попарно различные многочлены $c_i^2 - 4d_i < 0$ $(i = 1, \quad , t)$

Пусть $F = \mathbb{Q}$ Можно доказать, что неприводимыми над $\mathbb{Q}$ могут быть многочлены любой степени Например, многочлен $p(x) = x^n - 2$, неприводим при любом $n \geq 1$ Для доказательства этого утверждения и других подобных обычно применяют признаки (достаточные условия) неприводимости Наиболее известным из них является так называемый признак Эйзенштейна

Теорема 13 (критерий Эйзенштейна)

Пусть $f(x) \in \mathbb{Z}[x]$, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \; + \quad + a_1 x + a_0$

Предположим, что существует такое простое число p что

1 a_n не делится на p

2 $a_{n-1}, \quad , a_1, a_0$ делятся на p

3 a_0 не делится на p^2

Тогда $f(x)$ неприводим над $\mathbb{Q}$

Доказательство этой теоремы опирается на нижеследующие леммы Гаусса

Лемма 1

Если $f(x) \in \mathbb{Z}[x]$ неприводим над $\mathbb{Z}$ (т е $f(x) \neq f_1(x) f_2(x)$, где $f_i(x) \in \mathbb{Z}[x]$ $\deg f_i(x) > 0,\ i = 1, 2$), то $f(x)$ неприводим и над $\mathbb{Q}$

Опр Содержанием многочлена f (x) называется НОД всех его коэффициентов

Обозначение cont ($f(x)$)

Лемма 2

Пусть $f(x), g(x) \in \mathbb{Z}[x]$
Тогда cont ($f(x)\, g(x)$) = cont ($f(x)$) cont ($g(x)$)

Q Как найти корни многочлена? (и тем самым частично найти его каноническое разложение)

A Для поля $\mathbb{Q}$ ответ в следующей теореме

Теорема 14

Пусть $f(x) \in \mathbb{Z}[x],\ f(x) = a_n x^n + \quad + \ + a_1 x + a_0$

Если $p/q \in \mathbb{Q}$ – корень $f(x)$, причем НОД (p, q) = 1, то p – делитель a_0 q – делитель a_n

Замечание

Эта теорема дает очевидный алгоритм поиска всех рациональных корней данного многочлена $f(x) \in \mathbb{Q}[x]$

Доказательство

Имеем $f\left(p/q\right) = 0$, т е

$$a_n \left(p/q\right)^n + \quad + \ + a_1 \left(p/q\right) + a_0 = 0$$

Избавимся от знаменателей

$$a_n p^n + a_{n-1} p^{n-1} q + \qquad + a_1 p q^{n-1} + \ + a_0 q^n = 0$$

Или

$$a_n p^n = q(-a_{n-1} p^{n-1} - \qquad - a_1 p q^{n-2} - a_0 q^{n-1})$$

Следовательно, $a_n p^n$ делится на q Т к $НОД\left(p^n, q\right) = 1$ (это – следствие взаимной простоты p и q), то a_n делится на q (по соответствующему свойству взаимно простых чисел)

Аналогично доказывается, что a_0 делится на p

п. 3 Собственные значения и собственные векторы

Пусть φ - линейный оператор, матрица которого в нек-ром базисе $b_1, \ldots, b_n$ ($n = \dim V$) имеет диагональный вид:

$$A_\varphi = \begin{pmatrix} \lambda_1 & \ldots & 0 \\ \ldots & \ldots & \ldots \\ 0 & \ldots & \lambda_n \end{pmatrix}$$

Действие этого оператора на векторы следующее:

$$\varphi(b_1) = \lambda_1 b_1, \ \varphi(b_2) = \lambda_2 b_2, \ldots, \varphi(b_n) = \lambda_n b_n$$

Опр. Спектром линейного оператора φ называется мн-во всех его собственных значений.

Спектр называется простым, если он состоит из n различных значений ($n = \dim V$)

Теорема 7 (о диагонализируемости линейного оператора с простым спектром)

Если $\varphi : V \to V$ линейный оператор с простым спектром, то φ – диагонализируемый оператор.

Лемма

Пусть $\lambda_1, \dots, \lambda_k$ – попарно различные собственные значения линейного оператора $\varphi : V \to V$, а $x_1, \dots, x_k$ – соответствующие им собственные векторы

Тогда $x_1, \dots, x_k$ линейно независимы.

Доказательство

Пусть

$$l_1 x_1 + \dots + l_k x_k$$

Предположим, что утверждение леммы для числа векторов $< k$. Имеем:

$$0 = l_1 \varphi(x_1) + l_2 \varphi(x_2) + \dots + l_k \varphi(x_k) =$$
$$= l_1 \lambda_1 x_1 + l_2 \lambda_2 x_2 + \dots + l_k \lambda_k x_k$$

След-но, умножив первое рав-во на $-\lambda_1$, добавив ко второму, имеем:

$$l_2 (\lambda_2 - \lambda_1) x_2 + \dots + l_k (\lambda_k - \lambda_1) x_k = 0$$

По предположению $x_2, \dots, x_k$ линейно независимы, поэтому отсюда следует, что

$$l_2 (\lambda_2 - \lambda_1) = \dots = l_k (\lambda_k - \lambda_1) = 0$$

Т.к. $\lambda_2 \neq \lambda_1, \dots, \lambda_k \neq \lambda_1$, то $l_2 = \dots = l_k = 0$

Также $l_1 x_1 = 0$, значит $l_1 = 0$.

Доказательство теоремы 7

Спектр оператора содержит n различных собств

1.13 13. Скалярное произведение в вещественном векторном пространстве. Ортогональные векторы. Линейная независимость ортогональной системы ненулевых векторов.

§ 10. Векторные пространства над произвольным полем

п 1 Определения и примеры

Пусть V – нек-рое мн-во. Элементы V будем называть „векторами".

Пусть F – нек-рое поле, эл-ты к-рого назовем „скалярами"

Будем считать, что на V задано „сложение", т.е. нек-рая бинарная алгебраическая операция, $(a, b) \to a+b=c$ $(a, b, c \in V)$; и также определена операция бинарная „умножение вектора на скаляр" $(a, k) \to ka = d$ $(a, d \in V;\ k \in F)$

Опр. Пара (V, F) называется векторным пространством V над F, если:

1 $(V, +)$ – абелева группа (нулевой эл-т – это нулевой вектор, противоположный эл-т – противоположный вектор $-a$)

2 $k(a+b) = ka + kb$ для любых $a, b \in V$; $k \in F$

3 $(k+m)a = ka + ma$ для любых $a \in V$; $k, m \in F$

4 $(kl)a = k(la)$ для любых $a \in V$; $k, l \in F$

5 $1a = a$ для любого $a \in V$ (1 – единица поля F)

Примеры

1 V – мн-во „обычных" геометрических векторов, например, векторов плоскости, F – множ-во действительных чисел

2 $V = \mathbb{R}^n$, $F = \mathbb{R}$

3 $V = F^n$ – арифметическое n-мерное векторное пространство над полем F

4 $V = P$ – произвольное поле, F – нек-рое подполе поля P. Тогда P можно рассматривать как векторное пространство над F. Приведем конкретный пример:

$$P = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}, \quad F = \mathbb{Q}$$

Говорят, что поле P является расширением поля F. Итак, любое расширение данного поля может быть рассмотрено как векторное пространство над этим полем

5 V = мн-во всех функций $f: \mathbb{R} \to \mathbb{R}$, $F = \mathbb{R}$ (пространство функций).

Свойства операций в векторном пространстве V над полем F

1. $k \cdot 0 = 0$ для любого $k \in F$, где 0 – нулевой вектор

2 $0 \cdot a = 0$ для любого $a \in V$

3 $k(a-b) = ka - kb$ для любых $a, b \in V$; $k \in F$

4. $(k-l)a = ka - la$ для любых $a \in V$, $k, l \in F$

5 $(-k) \cdot a = k(-a) = -(ka)$ для любых $a \in V$; $k \in F$

Опр. Подмножество L векторного пространства V над полем F называется подпространством, если оно само образует векторное пространство над F

Пример

Пусть V – векторное пространство функций

$f\ \mathbb{R} \to \mathbb{R}$ над $\mathbb{R}$. Положим L – мн-во всех многочленов, т.е. функций вида

$$f(x) = a_n x^n + \ldots + a_1 x + a_0$$

где $a_n, \ldots, a_1, a_0$ – действительные числа, $a_n \neq 0$

Это мн-во L является подпространством V

<u>Теорема 0</u> (характеристический признак подпространства)

Подмножество L векторного пространства V явл. подпространством тогда и только тогда, когда:

1. L замкнуто отн. сложения векторов
2. L замкнуто отн. умножения векторов на скаляры

<u>Доказательство</u>

Непосредственное сравнение условий 1,2 с условиями в определении пространства

<u>Пример 1</u>

V – пространство всех бесконечных послед-тей $(a_1, a_2, \ldots, a_n, \ldots)$ с элементами из $\mathbb{R}$ (сложение и умножение на вещественные числа поэлементное)

L – подпространство всех финитных послед-тей $(a_1, a_2, \ldots, a_n, 0, 0, \ldots)$, т.е. послед-тей, у к-рых лишь конечное число эл-тов отлично от нуля.

<u>Пример 2</u>

V – мн-во всех многочленов с $\mathbb{R}$ коэф. ($\mathbb{R}[x]$)

$L_n = \{ f(x) = a_0 + a_1 x + \ldots + a_n x_n^n,\ a_n \neq 0 \}$ – не подпространство V, т.к. L_n не замкнуто отн. сложения (может уменьшиться степень многочлена)

$L_{\leq n} = \{ f(x) = a_0 + a_1 x + \ldots + a_n x_n^n \mid a_i \in \mathbb{R} \}$ – подпространство V

<u>Следствие</u>

Пересечение 2 подпространств является подпространством

п. 3 Собственные значения и собственные векторы

Пусть φ — линейный оператор, матрица которого в нек-ром базисе $b_1, \ldots, b_n$ ($n = \dim V$) имеет диагональный вид:

$$A_\varphi = \begin{pmatrix} \lambda_1 & \ldots & 0 \\ \ldots & \ldots & \ldots \\ 0 & \ldots & \lambda_n \end{pmatrix}$$

Действие этого оператора на векторы следующее:

$$\varphi(b_1) = \lambda_1 b_1, \ \varphi(b_2) = \lambda_2 b_2, \ldots, \varphi(b_n) = \lambda_n b_n$$

$$\det\begin{pmatrix} a_{11}-\lambda & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22}-\lambda & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn}-\lambda \end{pmatrix}$$

или

$$(-1)^n \lambda^n + \dots = 0$$

Это алгебраическое ур-ие n-ой степени. Из теории многочленов следует, что корней этого ур-ия не более n, значит собственных значений любого линейного оператора не более $n = \dim V$.

<u>Опр.</u> Пусть $\lambda \in F$ – нек-рое собственное значение линейного оператора $\varphi: V \to V$.

Мн-во всех собственных векторов, принадлежащих собственному значению λ вместе с нулевым вектором, образует подпр-во, называемое собственным подпр-вом, соответствующим собственному значению λ.

Это подпр-во есть $\operatorname{Ker}(\varphi - \lambda \mathcal{E})$, где $\mathcal{E}$ – тождественный линейный оператор (тождественное преобразование).

<u>Обозначение</u>

$$L_\lambda = \operatorname{Ker}(\varphi - \lambda \mathcal{E})$$

собственное подпр-во оператора $\varphi: V \to V$, соотв. собственному значению λ.

<u>Опр</u> Если линейный оператор $\varphi: V \to V$ в нек-ром базисе может быть задан диагональной матрицей, то говорят, что φ – диагонализируемый линейный оператор.

Легко видеть, что любой диагонализируемый оператор имеет $n = \dim V$ линейно независимых собственных векторов.

Обратно, если линейный оператор диагонализируемый, то он имеет n линейно независимые собственные векторы.

Опр. Спектром линейного оператора φ называется мн-во всех его собственных значений.

Спектр называется простым, если он состоит из n различных значений ($n = \dim V$)

Теорема 7 (о диагонализируемости линейного оператора с простым спектром)

Если $\varphi : V \to V$ линейный оператор с простым спектром, то φ – диагонализируемый оператор.

Лемма

Пусть $\lambda_1, \dots, \lambda_k$ – попарно различные собственные значения линейного оператора $\varphi : V \to V$, а $x_1, \dots, x_k$ – соответствующие им собственные векторы

Тогда $x_1, \dots, x_k$ линейно независимы.

Доказательство

Пусть

$$l_1 x_1 + \dots + l_k x_k$$

Предположим, что утверждение леммы для числа векторов $< k$. Имеем:

$$0 = l_1 \varphi(x_1) + l_2 \varphi(x_2) + \dots + l_k \varphi(x_k) =$$

$$= l_1 \lambda_1 x_1 + l_2 \lambda_2 x_2 + \dots + l_k \lambda_k x_k$$

След-но, умножив первое рав-во на $-\lambda_1$, добавив ко второму, имеем:

$$l_2(\lambda_2 - \lambda_1)x_2 + \dots + l_k(\lambda_k - \lambda_1)x_k = 0$$

По предположению $x_2, \dots, x_k$ линейно независимы, поэтому отсюда следует, что

$$l_2(\lambda_2 - \lambda_1) = \dots = l_k(\lambda_k - \lambda_1) = 0$$

Т.к. $\lambda_2 \neq \lambda_1, \dots, \lambda_k \neq \lambda_1$, то $l_2 = \dots = l_k = 0$
Также $l_1 x_1 = 0$, значит $l_1 = 0$.

Доказательство теоремы 7

Спектр оператора содержит n различных собств значений $\lambda_1, \dots, \lambda_n$. По лемме соотв. им собственные векторы $b_1, \dots, b_n$ будут линейно независимы и, след-но, их можно взять в кач-ве базиса V.

В этом базисе матрица оператора φ имеет диагональный вид.

$$A_\varphi = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

Если спектр оператора $\varphi\ V \to V$ не является простым, то оператор φ не обязательно недиагонализируемый.

<u>Пример</u>

$\varphi \cdot \mathbb{R}^3 \to \mathbb{R}^3$ задан матрицей

$$A_\varphi = \begin{pmatrix} -1 & 3 & -1 \\ -3 & 5 & -1 \\ -3 & 3 & 1 \end{pmatrix}$$

в нек-ром базисе b_1, b_2, b_3

Найдем собственные значения:

$$|A_\varphi - \lambda E| = \begin{vmatrix} -1-\lambda & 3 & -1 \\ -3 & 5-\lambda & -1 \\ -3 & 3 & 1-\lambda \end{vmatrix} = 0$$

$\lambda_1 = 1 \quad \lambda_2 = 2$

След-но оператор не имеет простого спектра.
Найдем собственные векторы:

1. $\lambda = 1$

$$\begin{pmatrix} -2 & 3 & -1 \\ -3 & 4 & -1 \\ -3 & 3 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\begin{cases} x_1 - x_2 = 0 \\ x_2 - x_3 = 0 \end{cases}$$

$L_{\lambda_1} = \langle (1, 1, 1) \rangle, \ \dim L_{\lambda_1} = 1$

2. $\lambda = 2$

$$\begin{pmatrix} -3 & 3 & -1 \\ -3 & 3 & -1 \\ -3 & 3 & -1 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$-3x_1 + 3x_2 - x_3 = 0$$

$$L_{\lambda_2} = \langle (1,1,0), (-1,0,3) \rangle, \dim L_{\lambda_2} = 2$$

Векторы $b_1' = (1,1,1)$, $b_2' = (1,1,0)$, $b_3' = (-1,0,3)$ образуют базис $\mathbb{R}^3$ и в этом базисе матрица оператора φ диагональна

$$A_\varphi' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

На диагонали матрицы находятся собственные значения $\lambda_1, \lambda_2, \lambda_3$.

Теорема 8 (критерий диагонализируемости)

Пусть линейный оператор $\varphi: V \to V$ имеет в точности k различных собственных значений $\lambda_1, \dots, \lambda_n$ $(k \le n = \dim V)$

Оператор φ диагонализируем тогда и только тогда, когда

$$\sum_{i=1}^{k} \dim L_{\lambda_i} = \dim V$$

Доказательство

$\Rightarrow$ Пусть φ — диагонализируемый оператор, т.е в нек-ром базисе его матрица имеет вид

$$A_\varphi = \begin{pmatrix} \underbrace{\lambda_1 \ddots \lambda_1}_{n_1} & & 0 \\ & \ddots & \\ 0 & & \underbrace{\lambda_k \ddots \lambda_k}_{n_k} \end{pmatrix}$$

Покажем, что собственное подпр-во L_{λ_i} $(i = 1, \dots, k)$ является линейной оболочкой тех базисных векторов, к-рые являются собственными с собственными значениями λ_i

Пусть $i = 1$, $L_{\lambda_1} = \langle b_1, \dots, b_{n_1} \rangle$. Предположим, что $x \in L_{\lambda_1}$ и

$$x = x_1 + \dots + x_k$$

где $x_1 \in \langle b_1, \dots, b_{n_1} \rangle, \dots, x_k \in \langle b_{n-n_k+1}, \dots, b_n \rangle$

Если, например, $x_2 \neq 0$, то было бы

$$\underset{\lambda_1}{(x_1 - x)} + \underset{\lambda_2}{x_2} + \underset{\dots}{\dots} + \underset{\lambda_k}{x_k} = 0$$

поэтому $x_2 = \dots = x_k = 0$, т.е. $x = x_1$

(по лемме о линейной независимости собственных векторов, соотв. различным собственным значениям)

Итак, $L_{\lambda_1} = \langle b_1, \dots, b_{n_1} \rangle$. В частности,

$$\dim L_{\lambda_i} = n_i \quad (i = 1, \dots, k)$$

Таким образом, сумма размерностей

$$\sum_{i=1}^{k} \dim L_{\lambda_i} = \sum_{i=1}^{k} n_i = n = \dim V.$$

$\Leftarrow$ Пусть

$$\sum_{i=1}^{k} \dim L_{\lambda_i} = n$$

Докажем, что

$$L_{\lambda_1} \oplus \dots \oplus L_{\lambda_k} = V$$

То, что сумма является прямой, есть следствие уже упомянутой леммы о линейной независимости, а тот факт, что она есть все пр-во V, вытекает из рав-ва $(*)$, т.к.

$$\dim (L_{\lambda_1} \oplus \dots \oplus L_{\lambda_k}) = \sum_{i=1}^{k} \dim L_{\lambda_i} = n$$

Взяв в каждом подпр-ве L_{λ_i} по базису и затем, соединив их, получим базис всего пр-ва V, в к-ром матрица оператора φ будет иметь диагональный вид

$$A_\varphi = \begin{pmatrix} \lambda_1 & & & & 0 \\ & \ddots & & & \\ & & \lambda_1 & & \\ & & & \ddots & \\ 0 & & & & \lambda_k \end{pmatrix}$$

1.14 14. Евклидово пространство. Матрица Грама скалярного произведения в базисе и её изменение при переходе к другому базису.

1.2 Линейная зависимость. Базис и ранг системы векторов

На общий случай без существенных изменений переносятся определения пропорциональных векторов, линейной комбинации векторов, тривиальной и нетривиальной линейных комбинаций, линейной выражаемости, линейной зависимости и независимости.

Опр. Векторы $a_1, \ldots, a_m \in V$ наз. линейно зависимыми, если существуют такие скаляры $k_1, \ldots, k_m \in F$, ~~что~~ не все равные нулю, что

$$k_1 a_1 + \ldots + k_m a_m = 0$$

Теорема 1 (признаки линейной зависимости)

Система векторов линейно зависима, если:

1. Содержит нулевой вектор.

2. Содержит линейно зависимую подсистему.

Теорема 2 (критерий линейной зависимости)

см Теорему 2 §3.

Теорема 3 (основная теорема о линейной зависимости)

см Теорему 3 §3.

Доказательство

аналогично, использует теорию СЛУ над произвольным полем в п. 4. §9

Следствие 1 (иная формулировка теоремы 3)

см Следствие 1 §3.

Следствие 2 теряет смысл.

Опр. Пусть $S: a_1, \ldots, a_m$ – конечная система векторов пространства V

Базисом S называется такая подсистема B, что:

1. B линейно независима;

2. S линейно выражается ч/з B

Теорема 4 (о существовании базиса конечной сист. вект.)

см Теорему 4 §3

Теорема 5 (о равномощности различных базисов данной системы векторов)

см Теорему 5 §3

Опр. Рангом системы S называется число векторов в любом ее базисе

Способ отыскания нек-рого базиса системы S, данный в §3 в общем случае не применим

Теорема 6 (о единственности разложения вектора по базису системы векторов)

см.

п. 3 Базис векторного пространства. Конечномерное векторное пространство

Опр. Пусть V - векторное пространство над полем F. Конечная система векторов B наз базисом V, если:

1. B линейно независима.

2. Любой вектор из V линейно выражается ч/з B.

Теорема 7 §3 для произвольного пр-ва не верна, т.к. существуют векторные пр-ва, не имеющие базиса:

Пусть V - векторное пр-во всех бесконечных финитных послед-ней из вещественных чисел

Покажем, что V не имеет базиса.

Пусть, напротив $B: b_1, \dots, b_n$ - нек-рый базис V.

Тогда:

$$b_1 = (b_{11}, \dots, b_{1m}, 0, 0, \dots)$$

$$b_2 = (b_{21}, \dots, b_{2m}, 0, 0, \dots)$$

$$\dots$$

$$b_n = (b_{n1}, \dots, b_{nm}, 0, 0, \dots)$$

где m - нек-рое натуральное число

Но в таком случае вектор

2) Пусть любые k лошадей 1 масти

1 2 3 4 5 6 7 8 k k+1

один. масть

один. масть — утверждение не для всех k верно

при k = 1

1 2

§3. Арифметическое n-мерное векторное пространство

1 Определения и примеры

Опр. Арифметический n-мерный вектор ~~векторное n-мерное пространство~~ — упорядоченный набор из n действительных чисел $a = (\alpha_1, \dots, \alpha_n)$

Пример.

1. Любое решение СЛУ с n неизвестными есть n-мерный арифметический вектор.

2. Пусть дана матрица размера $m \times n$. Тогда её строки — n-мерные арифметические векторы, столбцы — m-мерные арифметич. векторы.

Опр. α_i из арифметического n-мерного вектора $a = (\alpha_1, \dots, \alpha_n)$ называется компонентой этого вектора.

Опр. Два вектора $a = (\alpha_1, \dots, \alpha_n)$ и $b = (\beta_1, \dots, b_n)$ называются равными, если их соответствующие компоненты равны, т.е: $\alpha_i = \beta_i$ для всех $i = (1, \dots, n)$.

Это понятие верно только д/векторов одинаковой размерности.

Опр. Суммой двух векторов $a = (\alpha_1, \dots, \alpha_n)$ и $b = (\beta_1, \dots, \beta_n)$ называется вектор $c = (\gamma_1, \dots, \gamma_n)$, где $\gamma_i = \alpha_i + \beta_i$ для всех $i = (1, \dots, n)$.

Опр. Произведением вектора $a = (\alpha_1, \dots, \alpha_n)$ на число $k \in R$ называется вектор $d = (\delta_1, \dots, \delta_n)$, где $\delta_i = k \cdot \alpha_i$, $i = (1, \dots, n)$.

Опр. Нулевой вектор — вектор, всеми компонентами n-рого являются 0 ($0=(0,\dots,0)$)

Опр. Вектор, противоположный вектору $a=(\alpha_1,\dots,\alpha_n)$ — это вектор $(-\alpha_1,\dots,-\alpha_n)$. Он обозначается $-a$.

Опр. Разностью м/у векторами a и b называется вектор $(a+(-b))$.

Свойства операции сложение:

1. Для любых a, b имеем $a+b=b+a$. (коммутативность)
2. Для любых a, b, c $(a+b)+c=a+(b+c)$ (ассоциативность)

Свойство нулевого вектора:

Для любого a $a+0=a$

Свойство противоположного вектора

Для любого a $a+(-a)=0$

Свойства операции умножения вектора на число:

Для любого вектора a и числа α, β имеем $(\alpha\cdot\beta)a=\alpha\cdot\beta\cdot a$ (смешанная ассоциативность)

Для любого вектора a $1\cdot a=a$ (нормировка)

Свойства дистрибутивности

1. Для любого α и векторов a и b справедливо $\alpha(a+b)=\alpha a+\alpha b$
2. Для любых чисел α, β и вектора a имеем $(\alpha+\beta)a=\alpha a+\beta a$

Доказательства этих свойств вытекают из их определений и из аналогичных св-в операций над числами

Опр. Совокупность всех n-мерных арифметических векторов, рассматриваемая вместе с определенными в ней операциями сложения векторов и умножения векторов на число называется арифметическим n-мерным векторным пространством

Обозначение: $\mathbb{R}^n$

1. Линейная зависимость векторов в $\mathbb{R}^N$

Опр. Вектор $b \in \mathbb{R}^n$ называется пропорциональным вектору $a \in \mathbb{R}^n$, если $b = ka$, где $k \in \mathbb{R}$

Опр. Пусть дана система векторов $a_1, \dots, a_m \in \mathbb{R}^n$. Линейной комбинацией с коэффициентами $k_1, \dots, k_m$ этой системы векторов называется вектор вида $a = k_1 a_1 + \dots + k_m a_m \in \mathbb{R}^n$. Линейная комбинация называется тривиальной, если $k_1 = \dots = k_m = 0$ (тривиальная линейная комбинация есть нулевой вектор)

Опр. Линейно зависимая система — система векторов $a_1, a_2, \dots, a_m \in \mathbb{R}^n$, для которой существуют такие коэффициенты $k_1, \dots, k_m$, не все равные нулю, что $k_1 a_1 + \dots + k_m a_m = 0$

Иными словами, существует нетривиальная линейная комбинация векторов системы, равная нулевому вектору

R^2 — „плоскость" R^3 — „пространство"

Пример: R^3

$a_1 = (1, 0, -1)$

$a_2 = (2, -1, 0)$

$a_3 = (5, -2, -1)$

$a_1 + 2a_2 - a_3 = 0$

Действительно, $a_1 + 2a_2 - a_3 = (0, 0, 0)$

Эти векторы компланарны, т.е расположены в 1 плоскости

Опр. Линейно независимая система — система векторов $a_1, \dots, a_m \in \mathbb{R}^n$, к-рая не является линейно зависимой, по другому говоря, если из условия $k_1 a_1 + \dots + k_m a_m = 0$ следует, что $k_1 = \dots = k_m = 0$ (т.е. только тривиальная линейная комбинация этих векторов может быть равна нулевому вектору).

Типичная задача:

Для данной системы векторов выяснить, является ли она линейно зависимой, и если да, то предъявить нетривиальную комбинацию векторов системы, равную нулевому вектору

Пример $\mathbb{R}^3$

$a_1 = (1, 2, -1)$

$a_2 = (2, 1, 0)$

$a_3 = (1, 0, 0)$

Составляем линейную комбинацию этих векторов и приравниваем ее к нулевому вектору

$$k_1 a_1 + k_2 a_2 + k_3 a_3 = 0$$

Имеем

$$(k_1 + 2k_2 + k_3,\ 2k_1 + k_2,\ -k_1) = (0, 0, 0),$$

т.е.

$$\begin{cases} k_1 + 2k_2 + k_3 = 0, \\ 2k_1 + k_2 = 0, \\ -k_1 = 0; \end{cases}$$

эта однородная СЛУ имеет только нулевое решение, значит система векторов a_1, a_2, a_3 линейно независима.

Теорема 1 (признаки линейной зависимости)

Система векторов из $\mathbb{R}^n$ линейно зависима, если:

1) она содержит нулевой вектор;

2) она содержит линейно зависимую подсистему векторов.

Доказательство

1) Пусть система имеет вид $0, a_2, \ldots, a_m$. Тогда справедливо следующее соотношение:

$$1 \cdot 0 + 0 \cdot a_2 + \ldots + 0 \cdot a_m = 0$$

След-но, эта система линейно зависима.

2) Пусть система векторов имеет вид $a_1, \ldots, a_\ell, \ldots, a_m$, при этом система векторов $a_1, \ldots, a_\ell$ линейно зависима. Тогда существуют такие $k_1, \ldots, k_\ell$, не все равные нулю, что $k_1 a_1 + \ldots + k_\ell a_\ell = 0$. След-но, $k_1 a_1 + \ldots + k_\ell a_\ell + 0 a_{\ell+1} + \ldots + 0 a_m = 0$, т.е. нашлась нетривиальная линейная комбинация всех векторов системы, равная нулевому вектору.

~~Пример~~ 1 показывает, что условия 1) и 2) являются лишь достаточными, но не необходимыми.

Теорема 2 (критерий линейной зависимости)

Система векторов является линейно зависимой тогда и только тогда, когда один из векторов системы линейно выражается через остальные.

Примечание

Считаем, что в системе имеется хотя бы 2 вектора.

Вектор линейно выражается ч/з другие векторы, значит является их линейной комбинацией

Доказательство

$\Rightarrow$ Пусть система векторов $a_1, \dots, a_m$ линейно зависима. Тогда $k_1 a_1 + \dots + k_m a_m = 0$ для некоторых $k_1, \dots, k_m$, причем среди последних есть ненулевые. Пусть $k_1 \neq 0$. Тогда $a_1 = -\frac{k_2}{k_1} a_2 + \dots + (-\frac{k_m}{k_1}) a_m$.

$\Leftarrow$ Пусть, например, вектор a_1 линейно выражается ч/з векторы $a_2, \dots, a_m$:

$$a_1 = l_2 a_2 + \dots + l_m a_m$$

Тогда:

$$a_1 + (-l_2) a_2 + \dots + (-l_m) a_m = 0$$

Получена нетривиальная линейная комбинация всех векторов, равная нулевому вектору.

3 Основная теорема о линейной зависимости и ее следствия

Пусть в $\mathbb{R}^n$ даны 2 системы векторов:

$$S: a_1, \dots, a_m \quad (*)$$
$$T: b_1, \dots, b_s$$

Опр. Будем говорить, что система T линейно выражается ч/з систему S, если всякий вектор системы T линейно выражается ч/з векторы системы S

Лемма Если T линейно выражается ч/з S, а S линейно выражается ч/з R, то T линейно выражается ч/з R (T, S, R – 3 сист. вект. в $\mathbb{R}^n$)

Доказательство очевидно.

Теорема 3 (основная теорема о лин зависимости)

Пусть даны 2 системы векторов S и T (*)
Если $S > M$ и система T линейно выражается ч/з систему S, то система T линейно зависима.

Доказательство

Докажем, что существуют такие не все равные нулю коэффициенты $k_1, \dots, k_S$, что
$k_1 b_1 + \dots + k_S b_S = 0$

T линейно выражается ч/з S по условию, значит

$$b_1 = l_{11} a_1 + \dots + l_{1m} a_m$$

$$\dots$$

$$b_S = l_{S1} a_1 + \dots + l_{Sm} a_m$$

Имеем

$$k_1 b_1 + k_2 b_2 + \dots + k_S b_S =$$
$$= (l_{11} k_1 + l_{21} k_2 + \dots + l_{S1} k_S) a_1 +$$
$$+ (l_{12} k_1 + l_{22} k_2 + \dots + l_{S2} k_S) a_2 + \dots +$$
$$+ (l_{1m} k_1 + l_{2m} k_2 + \dots + l_{Sm} k_S) a_m = 0$$

Это равенство будет иметь место в случае, когда:

$$\begin{cases} l_{11} k_1 + \dots + l_{S1} k_S = 0, \\ \dots \\ l_{1m} k_1 + \dots + l_{Sm} k_S = 0, \end{cases} \quad (*)$$

Эту систему равенств можно рассматривать как однородную СЛУ с неизвестными $k_1, \dots, k_S$

Так как ур-ий m, а по условию $m < S$, то согласно теореме 4 §1 система (*) имеет ненулевое решения

Взяв произвольное ненулевое решение $(k_1, \dots, k_S)$ мы получим

$$k_1 b_1 + \dots + k_S b_S = 0$$

Следствие 1

Если система векторов из s векторов линейно независима и линейно выражается ч/з систему из m векторов, то $s \le m$.

Доказательство (от противного)

Если $s > m$, то по теореме 3 (основной теореме о линейной зависимости) система из S векторов будет линейно зависимой — противоречие с условием.

Следствие 2

В $\mathbb{R}^n$ любая система, состоящая более чем из n векторов будет линейно зависимой

Доказательство.

Пусть дана система векторов $b_1, \dots, b_s$, где $s > n$ (система T). В кач-ве системы S рассмотрим систему так называемых единичных векторов:

$e_1 = (1, 0, \dots, 0)$

$e_2 = (0, 1, 0, \dots, 0)$

$\dots$

$e_n = (0, 0, \dots, 1)$

Применим теорему 3, т.к. очевидно, что любой вектор из $\mathbb{R}^n$ можно выразить ч/з единичные векторы ($a = (a_1, a_2, \dots, a_n) = a_1 e_1 + a_2 e_2 + \dots + a_n e_n$).

По теореме 3 векторы $b_1, \dots, b_s$ линейно зависимы.

4 Базис

Опр. Пусть дана система векторов S пр-ва $\mathbb{R}^n$. Ее подсистема B называется базисом S, если:

1. B — линейно независимая система
2. S линейно выражается ч/з B

Пример $\mathbb{R}^3$

S: $a_1 = (1; 2; 1)$, $a_2 = (0; -1; 3)$, $a_3 = (2; 3; 1)$

Проверим, что подсистема B является базисом.

1) линейная незав
2) лин выр

1) Векторы a_1, a_2 не пропорциональны, поэтому независимы

2) $a_1 = 1 \cdot a_1 + 0 \cdot a_2$
$a_2 = 0 \cdot a_1 + 1 \cdot a_2$
$a_3 = 2a_1 + a_2$

Аналогично можно проверить, что подсистемы a_1, a_3; a_2, a_3 также будут базисами S.

Теорема 4 (о существовании базиса системы векторов)

Всякая система векторов S пр-ва $\mathbb{R}^n$ имеет базис (при этом не единственный)

Доказательство

Считаем, что в системе S есть ненулевые векторы.

Пусть $a \in S$ – один из них. Тогда система S имеет линейно независимые подсистемы (таковой будет, например, подсистема, образованная вектором $a \neq 0$)

Пусть B – линейно независимая подсистема S максимальной „длины".

Докажем, что B – базис S

1) B – линейно независимая подсистема по определению

2) Любой вектор из S линейно выражается через B

Пусть B $b_1, \ldots, b_r$, $a \in S$.

Докажем, что a линейно выражается ч/з $b_1, \ldots, b_r$

Для этого рассмотрим подсистему $B': b_1, \ldots, b_r, a$.

Эта подсистема линейно зависима, так как иначе противоречие с максимальностью подсистемы B

След-но $k_1 b_1 + \ldots + k_r b_r + ka = 0$ для нек-рых $k_1, \ldots, k_r, k$, не всех равных нулю.

Заметим, что $k \neq 0$ (иначе $k_1 b_1 + \ldots + k_r b_r = 0$, среди коэф есть ненулевой коэффициент — противоречие с линейной независимостью подсистемы B)

Тогда:

$$a = -{k_1}/{k}\, b_1 + \ldots + \left(-{k_r}/{k}\right) b_r,$$ т.е. a линейно выражается ч/з $b_1, \ldots, b_r$

След-но, подсистема B является базисом.

Теорема 5

Число векторов в разных базисах системы S одно и то же.

Доказательство

Пусть B_1, B_2 – два базиса системы S. Число векторов в B_1 есть m, число векторов в B_2 есть s

Так как B_2 линейно независима и линейно выражается через B_1 (так как B_1 – базис), то по следствию 1 теоремы 3 имеем $s \le m$

Меняя в этом рассуждении B_1 и B_2 местами получим, что $m \le s$.

След-но, $m = s$. ∎

Опр Рангом системы векторов S называется число векторов в любом ее базисе.

Обозначение $\operatorname{rank}(S)$ или $r(S)$.

Примечание

Если система векторов состоит только из нулевых векторов, то ее ранг равен нулю

Алгоритм отыскания некоторого базиса данной системы векторов S

Пусть S: $a_1, \ldots, a_m$

1. Составим линейную комбинацию из векторов $a_1, \ldots, a_m$ с коэффициентами $k_1, \ldots, k_m$ и приравняем ее к нулевому вектору: $k_1 a_1 + \ldots + k_m a_m = 0$
2. Заменим это векторное равенство эквивалентной системой обычных равенств. Пусть:

$$a_1 = (a_{11}, \ldots, a_{1n}),$$
$$\ldots$$
$$a_m = (a_{m1}, \ldots, a_{mn}).$$

Тогда:

$$\begin{cases} a_{11}k_1 + \ldots + a_{m1}k_m = 0 \\ \ldots \\ a_{1n}k_1 + \ldots + a_{mn}k_m = 0 \end{cases}$$

3. Приведем эту однородную СЛУ к ступенчатому виду.

4. В качестве базиса системы S можно взять подсистему тех векторов, номера к-рых суть номера главных неизвестных данной однородной СЛУ

<u>Пример</u> $\mathbb{R}^4$ $S: a_1, a_2, a_3, a_4, a_5$

$a_1 = (1, 2, 3, 4)$,

$a_2 = (0, 1, 0, 0)$,

$a_3 = (1, 1, 3, 4)$,

$a_4 = (0, 0, 1, 1)$,

$a_5 = (-1, -1, 2, 1)$.

$k_1 a_1 + \ldots + k_5 a_5 = 0$

$$\begin{cases} k_1 + k_3 - k_5 = 0, \\ 2k_1 + k_2 + k_3 - k_5 = 0, \\ 3k_1 + 3k_3 + k_4 + 2k_5 = 0 \\ 4k_1 + 4k_3 + k_4 + k_5 = 0 \end{cases}$$

$$\begin{pmatrix} 1 & 0 & 1 & 0 & -1 \\ 2 & 1 & 1 & 0 & -1 \\ 3 & 0 & 3 & 1 & 2 \\ 4 & 0 & 4 & 1 & 1 \end{pmatrix} \sim \ldots \sim \begin{pmatrix} 1 & 0 & 1 & 0 & -1 \\ 0 & 1 & -1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 5 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

a_1, a_2, a_4 (т.к. k_1, k_2, k_3 - глав. неизв) образуют базис системы S

Для того, чтобы выразить небазисные векторы ч/з базисные нужно решить однородную СЛУ

$$\begin{cases} k_1 = -k_3 + k_5 \\ k_2 = k_3 + k_5 \\ k_4 = -5k_5 \end{cases}$$

Проверим при a_3:

Положим $k_3 = 1$, $k_5 = 0$

Тогда:

$k_1 = -1$ $k_2 = 1$ $k_4 = 0$

$-1a_1 + a_2 + a_3 = 0$

$a_3 = a_1 - a_2$

Аналогично находится для a_5:

$a_5 = -a_1 - a_2 + 5a_4$

Обоснование $k_1a_1 + \ldots + k_m a_m = 0$

Допустим, что главными неизвестными оказались $k_1, \ldots, k_r$.

При этом
$$\begin{cases} k_1 = c_{1r+1}k_{r+1} + c_{2r+2}k_{r+2} + \ldots + c_{1m}k_m, \\ \ldots \\ k_r = c_{r,r+1} + \ldots + c_{rm}k_m; \end{cases} \quad (*)$$

Докажем, что векторы $a_1, \ldots, a_r$ образуют базис системы S

1) $a_1, \ldots, a_r$ линейно независимы

Пусть $l_1a_1 + \ldots + l_r a_r = 0$. Запишем это в виде $l_1a_1 + \ldots + l_r a_r + 0 \cdot a_{r+1} + \ldots + 0 \cdot a_m = 0$

Это ур-ие является частным случаем $k_1a_1 + \ldots + ka_r$, т.е числа $l_1, \ldots, l_r$ получаются по формулам $(*)$, если положить $k_{r+1} = \ldots = k_m = 0$, т.е числа $l_1, \ldots, l_r$ все равны нулю, т.к выражаются ч/з $k_{r+1}, \ldots, k_m$.

2). $a_{r+1}, \ldots, a_m$ линейно выражаются ч/з $a_1, \ldots, a_r$

Выразим, например a_m ч/з $a_1, \ldots, a_r$
Для этого положим $k_{r+1} = \ldots = k_{m-1} = 0$, $k_m = 1$. Тогда $k_1a_1 + \ldots + k_r a_r + a_m = 0$, где $k_1, \ldots, k_r$ — найденные по формулам $(*)$

Отсюда $a_m = (-k_1)a_1 + \ldots + (-k_r)a_r$

Итак, $a_1, \ldots, a_r$ — базис S.

Теорема 6

Разложение произвольного вектора системы S по ее базису единственно

Доказательство

Согласно условию 2 в определении базиса всякий вектор системы S допускает разложение по базису B

$a = k_1 b_1 + \ldots + k_r b_r,$

где a — вектор системы, $b_1, \ldots, b_r$ — базис B

Допустим, что имеется еще одно разложение

$a = k_1' b_1 + \ldots + k_r' b_r$

Тогда их разность равна:

$0 = (k_1 - k_1')b_1 + \ldots + (k_r - k_r')b_r$

Так как базис по определению линейно независимая система, то $k_1 - k_1' = \ldots = k_r - k_r' = 0$, следно $k_1 = k_1', \ldots, k_r = k_r'$.

Опр Базисом пространства $\mathbb{R}^n$ называется такая конечная система векторов B, что:

1) B — линейна независимая система

2) Любой вектор из $\mathbb{R}^n$ линейно выражается ч/з вектор B.

Теорема 7

Базисы пространства $\mathbb{R}^n$ существуют

Доказательство:

Рассмотрим систему единичных векторов

$e_1 = (1, 0, \ldots, 0)$
$e_2 = (0, 1, \ldots, 0)$
$\ldots$
$e_n = (0, 0, \ldots, 1)$

Докажем, что эта система явл. базисом, что очевидно ($k_1 + k_2 + \ldots + k_n = 0$, любой вектор выр ч/з един)

п. 6. Самосопряженные и ортогональные операторы в евклидовом пространстве

Предположим, что V – евклидово пространство Тогда V и V^* канонически изоморфны и эти пространства, следовательно, можно отождествить

Значит, можно считать, что сопряженный оператор φ^* действует в том же пространстве что и исходный оператор φ Таким образом, сопряженный оператор φ^* может быть определен так

$$(\varphi^*(y), x) = (y, \varphi(x)),$$

где $x, y \in V$ и внешние скобки обозначают операцию скалярного умножения, заданную в V

Если $a_1, \ldots, a_n$ – некоторый базис V, $a_1^*, \ldots, a_n^*$ – сопряженный базис V, т е

$$(a_i^*, a_j) = \begin{cases} 1, i = j, \\ 0, i \neq j \end{cases}$$

то матрица A_{φ^*} оператора φ^* в базисе, сопряженном $a_1^*, \ldots, a_n^*$, равна A_φ^t, где A_φ – матрица оператора φ в базисе $a_1, \ldots, a_n$

В случае ортонормированного базиса имеем $a_j^* = a_j$ (т е сопряженный базис совпадает с исходным) и переход к сопряженному оператору наиболее прост он состоит в транспонировании матрицы исходного оператора – $A_{\varphi^*} = A_\varphi^t$

Опр Оператор $\varphi\ V \to V$ называется самосопряженным (или симметричным) если

$$\varphi^* = \varphi$$

Для самосопряженных операторов имеем

$$(\varphi(y), x) = (y, \varphi(x))$$

где $x, y \in V$

В координатной форме условие самосопряженности выражается следующим образом $A_\varphi = A_\varphi^t$, т е матрица оператора φ в ортонормированном базисе является симметричной

Лемма

У самосопряженного оператора $\varphi\ V \to V$ есть вещественное собственное значение

Доказательство

Рассмотрим квадратичную функцию

$$q(x) = (\varphi(x), x),$$

где $x \in V$

На «сфере» $S = \{x \in V \mid |x| = 1\}$ эта функция $q(x)$ принимает минимальное значение (как и любая непрерывная на S функция)

$$\min_{x \in S} q(x) = \ = \min_{x \in S} (\varphi(x), x) = \ = \varphi(\varphi(x_0), x_0) = \ = q(x_0) = \lambda_0,$$

где $|x_0| = 1$

Положим $\psi = \varphi - \lambda_0 \varepsilon$ Имеем $(\psi(x), x) \geq 0$ для всех $x \in V$ Ясно что ψ – самосопряженный оператор Кроме того, $(\psi(x_0), x_0) = 0$

На самом деле, $\psi(x_0) = 0$, т е x_0 – собственный вектор с собственным значением λ_0

Пусть $\psi(x_0) \neq 0$, тогда $(\psi(x_0), y) \neq 0$ для некоторого $y \in V$

Рассмотрим вектор $x = x_0 + ty$ $(t \in \mathbb{R})$ Имеем

$$(\psi(x), x) = = (\psi(x_0) + t\psi(x_0), x_0 + ty) = = (\psi(x_0), x_0) + t(\psi(x_0), y) +$$
$$+t(\psi(y), x_0) + t^2(\psi(y), y) = = 2t(\psi(x_0), y) + +t^2(\psi(y), y) \geq 0$$

для всех t

Это невозможно, поскольку $(\psi(x_0), y) \neq 0$ – противоречие

Другое доказательство. Пусть A_φ – матрица самосопряженного оператора $\varphi: V \to V$ в каком-нибудь базисе. Характеристическое уравнение $\det(A_\varphi - \lambda E) = 0$ имеет комплексный корень $\lambda = \alpha + i\beta$. Пусть X – ненулевой столбец комплексных чисел, такой, что $A_\varphi X = \lambda X$. Положим $X = X_1 + iX_2$, где X_1, X_2 – вещественные столбцы; тогда

$$\begin{cases} A_\varphi X_1 = \alpha X_1 - \beta X_2, \\ A_\varphi X_2 = \beta X_1 + \alpha X_2 \end{cases}$$

Пусть $x_1, x_2 \in V$ – векторы со столбцами координат X_1, X_2 соответственно. Тогда

$$\begin{cases} \varphi(x_1) = \alpha x_1 - \beta x_2, \\ \varphi(x_2) = \beta x_1 + \alpha x_2 \end{cases}$$

Имеем $(\varphi(x_1), x_2) = (x_1, \varphi(x_2))$, что равносильно $\beta(|x_1|^2 + |x_2|^2) = 0$. Отсюда $\beta = 0$, т.е. $\lambda \in \mathbb{R}$.

Замечание. Попутно доказано, что линейный оператор $\varphi: V \to V$ в вещественном векторном пространстве V имеет либо одномерные, либо двумерные инвариантные подпространства (это $L = \langle x_1, x_2 \rangle$). При $\beta \neq 0$ векторы x_1, x_2 линейно независимы.

Лемма 2

Пусть L — инвариантное подпр-во относительно самосопряженного оператора $\varphi: V \to V$. Тогда $L^\perp$ также является инвариантным подпр-вом относительно φ.

Доказательство

Имеем $\varphi(L) \subset L$. Нужно док-ть, что из условия $x \in L^\perp$ следует, что $\varphi(x) \in L^\perp$.

Так как φ - самосопряженный оператор, то

$$(\varphi(u), v) = (u, \varphi(v))$$

для любых $u, v \in V$

Докажем, что $(\varphi(x), y) = 0$ для любого $y \in L$.
Действительно,

$$(\varphi(x), y) = (x, \varphi(y)) = 0$$

поскольку $x \in L^\perp$, а $\varphi(y) \in L$

Теорема 10

Пусть $\varphi: V \to V$ — самосопряженный оператор в евклидовом пр-ве V. Тогда существует ортонормированный базис, в к-ром матрица оператора φ диагональна

Доказательство

По Лемме 1 существует вектор $e_1 \in V$ единич. длины, к-рый является собственным для оператора $\varphi: V \to V$.

Значит, $L = \langle e_1 \rangle$ — инвариантное одномерное подпр-во

По Лемме 2 $L^\perp$ — инвариантное подпр-во, при этом $V = L \oplus L^\perp$

Рассматривая φ на подпр-ве $L^\perp$, размерность к-рого равна $n-1 < n$, и, рассуждая по индукции, найдем ортонормированный базис $e_2, \dots, e_n$ подпр-ва $L^\perp$, в к-ром матрица φ диагональна.

Тогда $e_1, \dots, e_n$ — ортонормированный базис V, в к-ром оператор φ задается диагональной матрицей.

Замечание

Собственные векторы самосопряженного оператора, соответствующие различным собственным значениям, образуют ортогональную систему.

Это следует из леммы 2, но также может быть доказано непосредственно

Пусть x, y – собственные векторы (принадлежащие ~~причем~~ λ_1, λ_2, причем $\lambda_1 \neq \lambda_2$

Имеем:

$$(\varphi(x), y) = (\lambda_1 x, y) = \lambda_1 (x, y)$$
$$\parallel$$
$$(y, \varphi(y)) = (x, \lambda_2 y) = \lambda_2 (x, y)$$

След-но,

$$(\lambda_2 - \lambda_1)(x, y) = 0$$

т.е.

$$(x, y) = 0$$

Опр. Линейный оператор $\varphi : V \to V$ евклидова пр-ва V называется ортогональным, если

$$(\varphi(x), \varphi(y)) = (x, y)$$

для любых $x, y \in V$.

Иными словами, ортогональное преобразование – это то, которое сохраняет скалярное произведение.

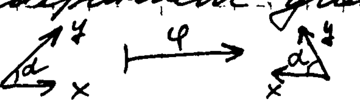
Можно показать, что д/ортогональности линейного оператора достаточно выполнения следующего условия:

$$|\varphi(x)| = |x|$$

для любого $x \in V$

Замечание

Ясно, что ортогональное преобразование сохраняет угол м/у векторами



п. 4. Нормальная жорданова форма

Если $x \in V$ – собственный вектор линейного оператора φ $V \to V$, подпространство L = <x> обладает следующим свойством инвариантности $\varphi(L) \subset L$, где $\varphi(L) = \{\varphi(x) \mid x \in L\}$ – образ подпространства L относительно действия оператора φ

Опр Подпространство L пространства V называется инвариантным относительно линейного оператора $\varphi(L) \subset L$, если $\varphi(L) \subset L$

Выберем в L базис b_1, $,b_n$ (n = dim L) и дополним его до базиса всего пространства V b_1, $,b_k, b_{k+1}$, $,b_n$ (n = dim L) В этом базисе матрица оператора φ имеет вид

$$A_\varphi = \begin{pmatrix} A_1 & A_0 \\ 0 & A_2 \end{pmatrix},$$

где A_1 – матрица порядка k

Предположим теперь, что $V = L_1 \oplus L_2$, где L_1 и L_2 – инвариантные подпространства Тогда в подходящем базисе (а именно, в базисе, полученном соединением базисов подпространств L_1 и L_2)

Матрица оператора φ имеет вид

$$A_\varphi = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$$

Опр Матрица вида

$$\begin{pmatrix} A_1 & & 0 \\ & A_2 & \\ & & \\ 0 & & A_m \end{pmatrix}$$

называется блочно-диагональной (блоки A_i (i = 1 m) – это квадратные матрицы порядка n_i, расположенные на главной диагонали, вне этих блоков находятся нули)

Таким образом, если имеет место разложение пространства V в прямую сумму нескольких инвариантных подпространств $V = L_1 \oplus \quad \oplus L_m$, где L_i (i = 1, , m) – инвариантное относительно φ подпространство, то матрица φ имеем блочно-диагональный вид

В частности, диагонализируемые операторы допускают разложение пространства V в прямую сумму одномерных инвариантных подпространств

Примеры

1 $\{0\}$, V – тривиальные инвариантные подпространства

2 $\operatorname{Ker}\varphi$, $\operatorname{Im}\varphi$ – инвариантные подпространства

3 Пусть оператор ψ $V \to V$ перестановочен с оператором φ, т е $\psi \circ \varphi = \varphi \ \psi$ тогда подпространства $\operatorname{Ker}\psi$, $\operatorname{Im}\psi$ инвариантные подпространства относительно действия оператора φ

1.15 15. Ортогональные и ортонормированные базисы в евклидовом пространстве. Процесс ортогонализации Грамма—Шмидта.

Теорема 5 (о равномощности различных базисов данной системы векторов)

см Теорему 5 §3

Опр. Рангом системы S называется число векторов в любом ее базисе

Способ отыскания нек-рого базиса системы S, данный в §3 в общем случае не применим

Теорема 6 (о единственности разложения вектора по базису системы векторов)

см.

п. 3 Базис векторного пространства. Конечномерное векторное пространство

Опр. Пусть V - векторное пространство над полем F. Конечная система векторов B наз базисом V, если:

1. B линейно независима.
2. Любой вектор из V линейно выражается ч/з B.

Теорема 7 §3 для произвольного пр-ва не верна, т.к. существуют векторные пр-ва, не имеющие базиса:

Пусть V - векторное пр-во всех бесконечных финитных послед-ней из вещественных чисел

Покажем, что V не имеет базиса.

Пусть, напротив $B: b_1, \ldots, b_n$ - нек-рый базис V.

Тогда:

$$b_1 = (b_{11}, \ldots, b_{1m}, 0, 0, \ldots)$$
$$b_2 = (b_{21}, \ldots, b_{2m}, 0, 0, \ldots)$$
$$\ldots$$
$$b_n = (b_{n1}, \ldots, b_{nm}, 0, 0, \ldots)$$

где m - нек-рое натуральное число

Но в таком случае вектор

$$b = (\underbrace{0, \ldots, 0}_{m}, 1, 0, 0, \ldots)$$

нельзя линейно выразить ч/з $b_1, \ldots, b_n$

Опр. Векторное пр-во V над полем F называется конечномерным, если оно обладает хотя бы одним базисом. В противном случае V называется бесконечномерным.

Примеры

1. $\mathbb{R}^n$ – конечномерное векторное пр-во над полем $\mathbb{R}$
2. F^n – конечномерное векторное пр-во над полем F
3. $\mathbb{R}[x]$ – бесконечномерное векторное пр-во многочленов от x с вещественными коэффициентами (по существу $\mathbb{R}[x]$ – пр-во финитных бесконечных послед-тей из вещественных чисел)

Теорема 8 (о равномощности базисов конечномерного векторного пространства)

Пусть V – конечномерное векторное пр-во над полем F

Тогда все базисы V содержат одно и то же число векторов.

Опр. Размерностью конечномерного векторного пространства V над полем F называется число векторов в любом его базисе

Обозначение $\dim V$

Пример $\dim \mathbb{R}^n = n$

Теорема 9 (о единственности разложения вектора пространства по его базису)

см Теорему 9 §3

Теорема 10

Пусть $\dim V = n$. Тогда любая система векторов, содержащая более чем n векторов является линейно зависимой (аналог следствия 2 теоремы 3 §3)

Утверждение

Векторное пр-во V бесконечномерно $\Leftrightarrow$ в V существуют сколь угодно длинные линейно независимые системы векторов.

Построение базиса конечномерного векторного пространства

Теорема 11 (о замене вектора в базисе)

Пусть $b_1, \dots, b_n$ – кон-рный базис пр-ва V. и вектор $a \in V$ таков, что $a = k_1 b_1 + \dots + k_n b_n$, $k_1 \neq 0$.

Тогда $a, b_2, \dots, b_n$ – также базис V.

Доказательство

1. Убедимся, что векторы $a, b_2, \dots, b_n$ ~~линейно~~ независимы.

Пусть $la + l_2 b_2 + \dots + l_n b_n = 0$, т.е

$$l(k_1 b_1 + \dots + k_n b_n) + l_2 b_2 + \dots + l_n b_n = 0$$

Имеем:

$$lk_1 b_1 + (lk_2 + l_2) b_2 + \dots + (lk_n + l_n) b_n = 0$$

След-но

$$lk_1 = 0$$
$$lk_2 + l_2 = 0$$
$$\dots$$
$$lk_n + l_n = 0$$

Т.к. по условию $k_1 \neq 0$, то из первого рав-ва следует, что $l = 0$. След-но из остальных рав-в имеем $l_2 = \dots = l_n = 0$

2. Докажем, что любой вектор $x \in V$ линейно выражается ч/з $a, b_2, \dots, b_n$

Для этого должны существовать коэф. $l, l_2, \dots, l_n$, такие, что:

$$x = la + l_2 b_2 + \dots + l_n b_n$$

Пусть

$$x = x_1 b_1 + \dots + x_n b_n$$

Тогда:

$$lk_1 b_1 + (lk_2 + l_2) b_2 + \dots + (lk_n + l_n) b_n =$$
$$= x_1 b_1 + \dots + x_n b_n$$

Т.к. $k_1 \neq 0$, имеем:

$$\ell = \frac{x_1}{k_1}, \ \ell_2 = x_2 - x_1\frac{k_2}{k_1}, \ldots, \ell_n = x_n - x_1\frac{k_n}{k_1}$$

Теорема 12 (о дополнении линейно независимой системы до базиса)

Пусть $b_1, \ldots, b_k$ – линейно независимая система векторов в n-мерном пространстве V.

Тогда существуют такие векторы $b_{k+1}, \ldots, b_n$, что $b_1, \ldots, b_n$ – базис V

Доказательство

Используем теорему о замене вектора в базисе.

Пусть $a_1, \ldots, a_n$ – нек-рый базис V

Так как $b_1 \neq 0$, то один из коэффициентов в его лин. выражении ч/з $a_1, \ldots, a_n$ не равен нулю.

Будем считать, что нулю не равен коэффициент при a_1.

Тогда возможно заменить вектор a_1 вектором b_1 в базисе, т.е. $b_1, a_2, \ldots, a_n$ – базис V

Разложим b_2 по этому базису.

$$b_2 = k_1 b_1 + k_2 a_2 + \ldots + k_n a_n$$

Среди коэффициентов $k_2, \ldots, k_n$ есть ненулевые, т.к. иначе векторы b_2 и b_1 пропорциональны, что противоречит линейной независимости $b_1, \ldots, b_k$

Пусть ненулевым коэффициентом является k_2

Тогда $b_1, b_2, a_3, \ldots, a_n$ – базис V по теореме 11

И т.д. в итоге получим базис $b_1, \ldots, b_k, a_{k+1}, \ldots, a_n$, что и требовалось доказать

Замечание

Эту теорему можно док-ть и другим способом (см док-во теоремы о существовании, которого нет и смотреть нечего)

Теорема 13

Если $b_1, \dots, b_n$ линейно независимы и $\dim V = n$, то $b_1, \dots, b_n$ — базис V

Доказательство

Предположим обратное, т.е. пусть существует вектор $a \in V$, к-рый невозможно линейно выразить ч/з $b_1, \dots, b_n$

Тогда $a, b_1, \dots, b_n$ — также линейно независимая система векторов — противоречие, т.к. $\dim V$ — максимально возможное число векторов в линейно независимой системе по Теореме 10.

Теорема 14 (о подпространстве конечномерного пространства)

Пусть L - подпространство V и $\dim V = n$.

Тогда L конечномерно и $\dim L \leq \dim V$

Если $\dim L = \dim V$, то $L = V$

Доказательство

L не может быть бесконечномерным, т.к иначе L имеет бесконечные линейно независимые подсистемы $\Rightarrow V$ также имеет бесконечные линейно независимые подсистемы $\Rightarrow V$ бесконечномерно — противоречие

Пусть $b_1, \dots, b_k$ — нек-рый базис L. По теореме 10 $k \leq n$, т.е $\dim L \leq \dim V$

Если $k = n$, по теореме 13 система $b_1, \dots, b_n$ явл. базисом V. Значит $L = V$

Опр. Пусть V, V' — векторные пространства над полем F. Пространства V и V' называются изоморфными, если существует такое отображение $\varphi: V \to V'$, что:

1. φ — биективное отображение,
2. $\varphi(a+b) = \varphi(a) + \varphi(b)$ и $\varphi(ka) = k\,\varphi(a)$ для любых $a, b \in V$, $k \in F$

Замечание

Это определение корректно (т.е симметрично по отношению к V, V'), т.к отображение

2) Пусть любые k лошадей 1 масти

$\underbrace{1\ 2\ 3\ 4\ 5\ 6\ 7\ 8 \ \dots\ k}_{\text{один. масть}}\ k+1$

$1\ \underbrace{2\ 3\ 4\ 5\ 6\ 7\ 8 \ \dots\ k\ k+1}_{\text{один. масть}}$ — утверждение не для всех k верно

при $k=1$

$\cdot\ \cdot$
1 2

§3. Арифметическое n-мерное векторное пространство

1 Определения и примеры

Опр. Арифметическое ~~векторное n-мерное пространство~~ n-мерный вектор — упорядоченный набор из n действительных чисел $a=(\alpha_1,\dots,\alpha_n)$

Пример.

1. Любое решение СЛУ с n неизвестными есть n-мерный арифметический вектор.
2. Пусть дана матрица размера $m\times n$. Тогда её строки — n-мерные арифметические векторы, столбцы — m-мерные арифметич. векторы.

Опр. α_i из арифметического n-мерного вектора $a=(\alpha_1,\dots,\alpha_n)$ называется компонентой этого вектора.

Опр Два вектора $a=(\alpha_1,\dots,\alpha_n)$ и $b=(\beta_1,\dots,b_n)$ называются равными, если их соответствующие компоненты равны, т.е.:
$\alpha_i=\beta_i$ для всех $i=(1,\dots,n)$.

Это понятие верно только д/векторов одинаковой размерности.

Опр. Суммой двух векторов $a=(\alpha_1,\dots,\alpha_n)$ и $b=(\beta_1,\dots,\beta_n)$ называется вектор $c=(\gamma_1,\dots,\gamma_n)$, где $\gamma_i=\alpha_i+\beta_i$ для всех $i=(1,\dots,n)$.

Опр. Произведением вектора $a=(\alpha_1,\dots,\alpha_n)$ на число $k\in R$ называется вектор $d=(\delta_1,\dots,\delta_n)$, где $\delta_i=k\cdot\alpha_i$, $i=(1,\dots,n)$.

Доказательство очевидно.

Теорема 3 (основная теорема о лин зависимости)
Пусть даны 2 системы векторов S и T (*)
Если $S > M$ и система T линейно выражается ч/з систему S, то система T линейно зависима.

Доказательство

Докажем, что существуют такие не все равные нулю коэффициенты $k_1, \ldots, k_S$, что
$k_1 b_1 + \ldots + k_S b_S = 0$

T линейно выражается ч/з S по условию, значит

$$b_1 = l_{11} a_1 + \ldots + l_{1m} a_m$$

$$\ldots$$

$$b_S = l_{S1} a_1 + \ldots + l_{Sm} a_m$$

Имеем

$$k_1 b_1 + k_2 b_2 + \ldots + k_S b_S =$$
$$= (l_{11} k_1 + l_{21} k_2 + \ldots + l_{S1} k_S) a_1 +$$
$$+ (l_{12} k_1 + l_{22} k_2 + \ldots + l_{S2} k_S) a_2 + \ldots +$$
$$+ (l_{1m} k_1 + l_{2m} k_2 + \ldots + l_{Sm} k_S) a_m = 0$$

Это равенство будет иметь место в случае, когда:

$$\begin{cases} l_{11} k_1 + \ldots + l_{S1} k_S = 0, \\ \ldots \\ l_{1m} k_1 + \ldots + l_{Sm} k_S = 0, \end{cases} \quad (*)$$

Эту систему равенств можно рассматривать как однородную СЛУ с неизвестными $k_1, \ldots, k_S$

Так как ур-ий m, а по условию $m < S$, то согласно теореме 4 §1 система (*) имеет ненулевое решения

Взяв произвольное ненулевое решение $(k_1, \ldots, k_S)$ мы получим

$$k_1 b_1 + \ldots + k_S b_S = 0$$

Следствие 1

Если система векторов из s векторов линейно независима и линейно выражается ч/з систему из m векторов, то $s \le m$.

Доказательство (от противного)

Если $s > m$, то по теореме 3 (основной теореме о линейной зависимости) система из S векторов будет линейно зависимой — противоречие с условием.

Следствие 2

В $\mathbb{R}^n$ любая система, состоящая более чем из n векторов будет линейно зависимой

Доказательство.

Пусть дана система векторов $b_1, \dots, b_s$, где $s > n$ (система T). В кач-ве системы S рассмотрим систему так называемых единичных векторов:

$$e_1 = (1, 0, \dots, 0)$$

$$e_2 = (0, 1, 0, \dots, 0)$$

$$\dots$$

$$e_n = (0, 0, \dots, 1)$$

Применим теорему 3, т.к. очевидно, что любой вектор из $\mathbb{R}^n$ можно выразить ч/з единичные векторы $(a = (a_1, a_2, \dots, a_n) = a_1 e_1 + a_2 e_2 + \dots + a_n e_n)$.

По теореме 3 векторы $b_1, \dots, b_s$ линейно зависимы.

4 Базис

Опр. Пусть дана система векторов S пр-ва $\mathbb{R}^n$. Ее подсистема B называется базисом S, если:

1. B — линейно независимая система
2. S линейно выражается ч/з B

Пример $\mathbb{R}^3$

S: $a_1 = (1; 2; -1)$, $a_2 = (0; -1; 3)$, $a_3 = (2; 3; 1)$

Проверим, что подсистема B является базисом.

1) линейная незав
2) лин выр

Отсюда $a_m = (-k_1)a_1 + \ldots + (-k_r)a_r$

Итак, $a_1, \ldots, a_r$ – базис S.

Теорема 6

Разложение произвольного вектора системы S по ее базису единственно

Доказательство

Согласно условию 2 в определении базиса всякий вектор системы S допускает разложение по базису B

$a = k_1 b_1 + \ldots + k_r b_r$,

где a – вектор системы, $b_1, \ldots, b_r$ – базис B

Допустим, что имеется еще одно разложение

$a = k_1' b_1 + \ldots + k_r' b_r$

Тогда их разность равна:

$0 = (k_1 - k_1')b_1 + \ldots + (k_r - k_r')b_r$

Так как базис по определению линейно независимая система, то $k_1 - k_1' = \ldots = k_r - k_r' = 0$, Следно $k_1 = k_1', \ldots, k_r = k_r'$.

Опр Базисом пространства $\mathbb{R}^n$ называется такая конечная система векторов B, что:

1) B – линейно независимая система

2) Любой вектор из $\mathbb{R}^n$ линейно выражается ч/з вектор B.

Теорема 7

Базисы пространства $\mathbb{R}^n$ существуют

Доказательство:

Рассмотрим систему единичных векторов

$e_1 = (1, 0, \ldots, 0)$
$e_2 = (0, 1, \ldots, 0)$
$\ldots$
$e_n = (0, 0, \ldots, 1)$

Докажем, что эта система явл. базисом, что очевидно ($k_1 + k_2 + \ldots + k_n = 0$, любой вектор выр ч/з един)

Пример. $\mathbb{R}^3$

$$\left.\begin{array}{l} a_1 = (1,2,1) \\ a_2 = (0,1,2) \\ a_3 = (0,0,-1). \end{array}\right\} B$$

Проверим, что B — базис $\mathbb{R}^3$.

1) $k_1a_1 + k_2a_2 + k_3a_3 = 0 \Leftrightarrow$

$$\begin{cases} k_1 = 0, \\ 2k_1 + k_2 = 0, \\ k_1 + 2k_2 - k_3 = 0 \end{cases} \Leftrightarrow k_1 = k_2 = k_3 = 0$$

2) $a \in \mathbb{R}^3$, $a = (\alpha_1, \alpha_2, \alpha_3)$

$k_1a_1 + k_2a_2 + k_3 = \alpha \Leftrightarrow$

$$\begin{cases} k_1 = \alpha_1, \\ 2k_1 + k_2 = \alpha_2, \\ k_1 + 2k_2 - k_3 = \alpha_3; \end{cases} \Leftrightarrow \begin{cases} k_1 = \alpha_1, \\ k_2 = \alpha_2 - 2\alpha_1, \\ k_3 = -\alpha_3 + 2\alpha_2 - 3\alpha_1 \end{cases}$$

След-но B — базис

Теорема 8

Любой базис пространства $\mathbb{R}^n$ состоит из n векторов

Доказательство

см. док-во теоремы 5

Опр. Размерностью пространства $\mathbb{R}^n$ называется число векторов в любом его базисе, т.е n

Теорема 9

Пусть B — фиксированный базис пространства $\mathbb{R}^n$. Тогда любой вектор a пространства $\mathbb{R}^n$ имеет единственное разложение по базису B...

Доказательство

см док-во теоремы 6

Замечание

Собственные векторы самосопряженного оператора, соответствующие различным собственным значениям, образуют ортогональную систему.

Это следует из леммы 2, но также может быть доказано непосредственно.

Пусть x, y – собственные векторы, принадлежащие λ_1, λ_2, причем $\lambda_1 \neq \lambda_2$

Имеем:

$$(\varphi(x), y) = (\lambda_1 x, y) = \lambda_1 (x, y)$$

$$\parallel$$

$$(y, \varphi(y)) = (x, \lambda_2 y) = \lambda_2 (x, y)$$

След-но,

$$(\lambda_2 - \lambda_1)(x, y) = 0$$

т.е.

$$(x, y) = 0$$

Опр. Линейный оператор $\varphi: V \to V$ евклидова пр-ва V называется ортогональным, если

$$(\varphi(x), \varphi(y)) = (x, y)$$

для любых $x, y \in V$.

Иными словами, ортогональное преобразование – это то, которое сохраняет скалярное произведение.

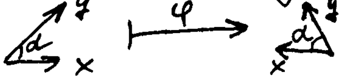
Можно показать, что д/ортогональности линейного оператора достаточно выполнения следующего условия:

$$|\varphi(x)| = |x|$$

для любого $x \in V$

Замечание

Ясно, что ортогональное преобразование сохраняет угол м/у векторами



Ортогональный оператор характеризуется также тем, что произвольный ортонормированный базис переводит в ортонормированный базис.

Поэтому переход от ортонормированного базиса к другому ортонормированному базису описывается ортогональной матрицей, то матрица ортогонального оператора в ортогональном базисе должна быть ортогональной ($A^{-1} = A^{t}$)

Предположим, что e – собственный вектор ортогонального оператора $\varphi : V \to V$. Тогда

$$\varphi(e) = \lambda e$$

и

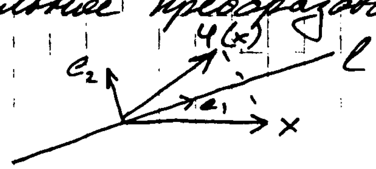
$$|\varphi(e)| = |\lambda||e| = |e|$$

т.е.

$$|\lambda| = 1, \quad \lambda = \pm 1$$

Примеры

1. Симметрия относительно оси – ортогональное преобразование плоскости.



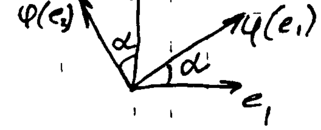
В ортонормированном базисе e_1, e_2 это преобразование задается матрицей

$$A_\varphi = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

2 Поворот вокруг начала координат на угол φ – ортогональное преобразование плоскости.

В ортонормированном базисе e_1, e_2 это преобразование может быть задано матрицей:

$$A_\varphi = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$



Если $\alpha \neq \pi + 2\pi k$ (т.е. поворот не явл. центральной симметрией), то собственных векторов нет. Иначе собственными будут все векторы.

ЗАМЕЧАНИЕ

Заметим, что других ортогональных преобразований плоскости нет. (док-ть).

Ортогональные преобразования, сохраняющие ориентацию пр-ва, называются собственными. Если ориентация пр-ва меняется, то говорят о несобственном ортогональном преобразовании.

Собственные ортогональные преобразования характеризуются тем, что их определитель равен $+1$, а несобственные — тем, что их определитель равен -1.

Опр. Определитель линейного оператора — это определитель его матрицы в каком-либо базисе.

Теорема 11

Пусть $\varphi: V \to V$ — ортогональный оператор в евклидовом пр-ве V. Тогда в нек-ром ортонормированном базисе матрица φ имеет вид.

$$\begin{pmatrix}
1 & & & & & & & & & \\
 & \ddots & & & & & & & 0 & \\
 & & 1 & & & & & & & \\
 & & & -1 & & & & & & \\
 & & & & \ddots & & & & & \\
 & & & & & -1 & & & & \\
 & & & & & & \cos\alpha_1 & -\sin\alpha_1 & & \\
 & 0 & & & & & \sin\alpha_1 & \cos\alpha_1 & & \\
 & & & & & & & & \ddots & \\
 & & & & & & & & \cos\alpha_k & -\sin\alpha_k \\
 & & & & & & & & \sin\alpha_k & \cos\alpha_k
\end{pmatrix}$$

ЗАМЕЧАНИЕ О ДОК-ВЕ

Док-во может быть получено на базе аналога лемм 1 и 2, а именно можно показать, что лемма 2 остается справедливой и д/ ортогонального преобразования, а Лемму 1 следует переформулировать след. образом: Любое ортогональное преобразование имеет либо одномерное, либо двумерное инвариантное подпр-во (это верно и д/ любых линейных преобразований).

1.16 16. Длина вектора, угол между векторами, угол между вектором и подпространством, объём параллелепипеда в евклидовом пространстве.

Теорема 13

Если $b_1, \dots, b_n$ линейно независимы и $\dim V = n$, то $b_1, \dots, b_n$ — базис V

Доказательство

Предположим обратное, т.е. пусть существует вектор $a \in V$, к-рый невозможно линейно выразить ч/з $b_1, \dots, b_n$

Тогда $a, b_1, \dots, b_n$ — также линейно независимая система векторов — противоречие, т.к. $\dim V$ — максимально возможное число векторов в линейно независимой системе по Теореме 10.

Теорема 14 (о подпространстве конечномерного пространства)

Пусть L - подпространство V и $\dim V = n$

Тогда L конечномерно и $\dim L \leq \dim V$

Если $\dim L = \dim V$, то $L = V$

Доказательство

L не может быть бесконечномерным, т.к иначе L имеет бесконечные линейно независимые подсистемы $\Rightarrow V$ также имеет бесконечные линейно независимые подсистемы $\Rightarrow V$ бесконечномерно — противоречие

Пусть $b_1, \dots, b_k$ — нек-рый базис L. По теореме 10 $k \leq n$, т.е $\dim L \leq \dim V$

Если $k = n$, по теореме 13 система $b_1, \dots, b_n$ яв. базисом V. Значит $L = V$

Опр. Пусть V, V' — векторные пространства над полем F. Пространства V и V' называются изоморфными, если существует такое отображение $\varphi: V \to V'$, что:

1. φ — биективное отображение,
2. $\varphi(a+b) = \varphi(a) + \varphi(b)$ и $\varphi(ka) = k\,\varphi(a)$ для любых $a, b \in V$, $k \in F$

Замечание

Это определение корректно (т.е симметрично по отношению к V, V'), т.к отображение

$\varphi^{-1}: V' \to V$ обратное отображение φ, также удовлетворяет условию #2

Будем называть φ отображением, осуществляющим изоморфизм м/у V и V'

Отношение „быть изоморфными" является отношением эквивалентности, т.е

1. V изоморфно V
2. Если V изоморфно V', то V' изоморфно V
3. Если V изоморфно V', V' изоморфно V'', то V изоморфно V'' (если φ, ψ – отображения, осуществляющие изоморфизм м/у V и V', V' и V'' соответственно, то $\varphi \circ \psi$ осуществляет изоморфизм м/у V и V'').

Теорема 15

Конечномерные пространства V и V' изоморфны тогда и только тогда, когда $\dim V = \dim V'$

Конечномерное и бесконечномерное пространства не могут быть изоморфны.

Доказательство

Отметим св-ва ~~изо~~отображения, осуществляющего изоморфизм м/у V и V':

1. $\varphi(0) = 0$
2. $\varphi(-a) = -\varphi(a)$ для любого $a \in V$
3. $\varphi(k_1 a_1 + \dots + k_m a_m) = k_1 \varphi(a_1) + \dots + k_m \varphi(a_m)$

Док-во этих св-в – непосредственное следствие условий 1–2 определения изоморфности.

Из этих св-в следует, в частности, что при изоморфизме линейно зависимые (независимые) системы векторов переходят в линейно зависимые (независимые) системы

$\Leftarrow$ Пусть $\dim V = \dim V' = n$

Построим изоморфизм $\varphi: V \to V'$

Выберем в V и V' по базису:

$b_1, \dots, b_n$ – базис V, $b_1', \dots, b_n'$ – базис V'

Определим отображение φ след. образом: если $x = x_1 b_1 + \dots + x_n b_n \in V$, то положим $\varphi(x) = x_1 b_1' + \dots + x_n b_n'$

Легко проверить, что $\varphi(x+y) = \varphi(x) + \varphi(y)$ и $\varphi(kx) = k\varphi(x)$ для любых $x, y \in V$, $k \in F$

Таким образом, т.к. также φ биективно, V изоморфно V'

$\Leftarrow$ Пусть теперь V и V' изоморфны и $\dim V = n$

Докажем, что $\dim V' = n$. Рассмотрим произвольный базис пространства V:

$b_1, \dots, b_n$

Тогда

$\varphi(b_1, \dots, b_n)$ –

базис пр-ва V' (следствие св-в изоморфизма, приведенных выше).

След-но $\dim V' = n = \dim V$.

Бесконечномерное пр-во не может быть изоморфно конечномерному, т.к. при изоморфизме линейно независимые системы переходят в линейно независимые, а в бесконечномерном пр-ве существуют сколь угодно длинные лин. незав. системы, в то время как в конечномерном пр-ве число векторов в линейно независимой системе векторов ограничено сверху его размерностью.

<u>Следствие</u>

Всякое n-мерное векторное пр-во V над полем F изоморфно n-мерному арифметическому пр-ву F^n.

<u>Пример</u>

1 $V = \mathbb{R}[x]$, V' = векторное пр-во бесконечных финитных послед-тей из вещественных чисел. Эти пространства изоморфны. Отображение $\varphi: V \to V'$ устроено след. обр.:

$$\varphi(a_0 + a_1 x + \dots + a_n x^n) = (a_0, a_1, \dots, a_n, 0, \dots)$$

2. $V_n = \{ f(x) \in \mathbb{R}[x] \mid \deg f(x) \le n \}$

(если $f(x) = a_0 + a_1 x + \dots + a_n x^n$, $a_n \neq 0$, то $\deg f(x) = n$)

V_n изоморфно $V' = \mathbb{R}^{n+1}$. Здесь $\varphi(a_0 + a_1 x + \dots + a_n x^n) = (a_0, a_1, \dots, a_n)$

3 Координаты вектора в базисе

Пусть V – нек-рое n-мерное векторное пространство над полем F.

Опр. Координатами вектора $a \in V$ в базисе $b_1, \dots, b_n$ называются коэффициенты в разложении

$$a = k_1 b_1 + \dots + k_n b_n$$

При фиксированном базисе каждому вектору $a \in V$ однозначно сопоставляется набор координат, к-рые записываются в виде столбца

$$a \to \begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix} = (k_1, \dots, k_n)^t$$

Это сопоставление согласовано с операциями над векторами: при сложении векторов их столбцы складываются, а при умножении вектора на скаляр столбец координат умножается на скаляр.

Пример

Рассмотрим $\mathbb{R}^n$, где в кач-ве базиса взят стандартный базис (базис из единичных векторов).

$e_1 = (1, 0, \dots, 0)$

$e_2 = (0, 1, \dots, 0)$

...

$e_n = (0, 0, \dots, 1)$

Тогда столбец координат произвольного вектора

$a = (a_1, \dots, a_n)$

есть $\begin{pmatrix} a_1 \\ a_n \end{pmatrix}$

§ 15. Билинейные и квадратичные функции

п. 1 Билинейные и квадратичные функции

Пусть V — векторное пр-во над полем F

Опр. Функция $g: V \times V \to F$ называется билинейной, если она линейна по каждому аргументу (при фиксированном другом):

$$g(k_1 x_1 + k_2 x_2, y) = k_1 g(x_1, y) + k_2 g(x_2, y)$$
$$g(x, l_1 y_1 + l_2 y_2) = l_1 g(x, y_1) + l_2 g(x, y_2)$$

Будем рассматривать только симметричные билинейные ф-ии, т.е.

$$g(x, y) = g(y, x) \qquad x, y \in V$$

Такие билинейные ф-ии наз. скалярными произведениями. Пр-во V, на к-ром задано такое скалярное произведение наз. пр-вом с ортогональной геометрией

Опр. Векторы $x, y \in V$, где V — пр-во с ортогональной геометрией, называются ортогональными, если $g(x, y) = 0$

Типичный пример пр-ва с ортогональной геометрией — евклидово пр-во над полем $\mathbb{R}$, скалярное произведение g в к-ром характеризуется доп. условием положительности:

$$g(x, x) > 0$$

для всех $x \neq 0$.

Опр. Функция $q: V \to F$ называется квадратичной, если

$$q(x) = g(x, x)$$

где g — нек-рая симметричная билинейная ф-ия (скалярное произведение) наз. поляризацией q.

Замечание

Если характеристика поля F ($\operatorname{char} F$) отлична от 2 (т.е $1+1\neq 0$), то существует единственная поляризация данной квадратичной ф-ии, а именно

$$g(x,y)=\frac{1}{2}\left(q(x+y)-q(x)-q(y)\right)$$

(вспомним тождество: $xy=\frac{1}{2}\left((x+y)^2-x^2-y^2\right)$)

Действительно, если

$$g_1(x,x)=g_2(x,x)$$

для всех $x\in V$, где g_1, g_2 — скалярные произведения, то

$$\tilde{g}(x,x)=0$$

для всех $x\in V$, где $\tilde{g}=g_1-g_2$

Но тогда

$$\tilde{g}(x,y)=0$$

для любых $x,y\in V$, что следует из рав-ва

$$0=\tilde{g}(x+y,x+y)=\tilde{g}(x,x)+2\tilde{g}(x,y)+\tilde{g}(y,y)=$$
$$=2\tilde{g}(x,y)$$

Таким образом,

$$\tilde{g}\equiv 0$$

т.е. $g_1=g_2$

Пусть $e_1,\dots,e_n$ — нек-рый базис V, g — скалярное произведение в V, $(x_1,\dots,x_n)^t$, $(y_1,\dots,y_n)^t$ — столбцы координат векторов $x,y\in V$.

Имеем:

$$g(x,y)=g(x_1e_1+\dots+x_ne_n,\ y_1e_1+\dots+y_ne_n)=$$
$$=\sum_{i=1}^{n}\sum_{j=1}^{n} g_{ij}\,x_i y_j$$

где $g_{ij}=(e_i,e_j)$. $(i,j=1,\dots,n)$.

Или:

$$g(x,y) = (x_1 \dots x_n)\, G \begin{pmatrix} y_1 \\ \dots \\ y_n \end{pmatrix}$$

где $G = (g_{ij})$ – матрица Грама скалярного произведения g в базисе $e_1, \dots, e_n$.

В частности,

$$g(x,x) = q(x) = (x_1 \dots x_n)\, G \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \sum_{i,j=1}^{n} g_{ij} x_i x_j$$

<u>Опр.</u> Выражения $\sum_{i,j=1}^{n} g_{ij} x_i y_j$ и $\sum_{i,j=1}^{n} g_{ij} x_i x_j$ называются, соответственно, билинейной и квадратичной формами. (от переменных $x_1, \dots, x_n, y_1, \dots, y_n$ в первом случае и $x_1, \dots, x_n$ во втором).

Пусть $e_1', \dots, e_n'$ – другой базис V и T – матрица перехода к нему. Тогда:

$$(e_1' \dots e_n') = (e_1 \dots e_n)\, T$$

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = T \begin{pmatrix} y_1' \\ \vdots \\ y_n' \end{pmatrix} \qquad (x_1 \dots x_n) = (x_1' \dots x_n')\, T^t$$

$$g(x,y) = (x_1 \dots x_n)\, G \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = (x_1' \dots x_n')\, T^t G T \begin{pmatrix} y_1' \\ \vdots \\ y_n' \end{pmatrix}$$

$$= (x_1' \dots x_n')\, G' \begin{pmatrix} y_1' \\ \dots \\ y_n' \end{pmatrix}$$

где $G' = T^t G T$ – матрица Грама в новом базисе $e_1', \dots, e_n'$.

<u>Опр.</u> Рангом скалярного произведения g наз. $\mathrm{rank}(G)$, где G – матрица Грама в нек-ром базисе пр-ва V. g наз. невырожденным, если его ранг равен $n = \dim V$.

<u>Замечание</u>

Определения ранга и невырожденности скалярного произведения корректны, т.е. не зависят от выбора базиса.

Это следует из ф-лы $G' = T^t G T$ и утверждения о том, что при умножении на невырожденную матрицу ранг матрицы не меняется.

Опр. Ядром скалярного произведения g называется подпр-во

$$\ker g = \{x \in V \mid g(x,y) = 0 \quad \forall y \in V\}.$$

Теорема 1

$$\dim \operatorname{Ker} g + \operatorname{rank} g = n$$

Доказательство

Пусть $e_1, \dots, e_n$ — лин-рый базис V. Тогда

$$\operatorname{Ker} g = \{x \in V \mid g(x, e_j) = 0,\ j = 1, \dots, n\}$$

В координатах $\operatorname{Ker} g$ задается ОСЛУ:

$$\sum_{i=1}^{n} g_{ij} x_i = 0; \quad j = 1, \dots, n$$

Очевидно, число свободных неизвестных этой системы есть $\dim \operatorname{Ker} g$, а число главных неизвестных есть $\operatorname{rank} g = \operatorname{rank} G$

Отсюда и следует утверждение теоремы.

Следствие

Скалярное произведение g невырожденно $\Leftrightarrow \operatorname{Ker} g = \{0\}$

.2 Ортогональные базисы

Опр. Ортогональным дополнением подпр-ва пр-ва V относительно g наз. подпр-во

$$L^{\perp} = \{x \in V \mid g(x,y) = 0 \quad \forall y \in L\}$$

В частности, $\operatorname{Ker} g = V^{\perp}$.

Опр. Подпр-во L пр-ва V называется невырожденным отн. скалярного произведения g, если сужение g на L является невырожденным скалярным произведением на L.

Опр. Подпр-во L пр-ва V наз. изотропным, если сужение g на L является тождественно нулевым, т.е.

$$g(x,y) = 0$$

для любых $x, y \in L$.

Замечание

Ясно, что $\operatorname{Ker} g$ – изотропное подпр-во

Даже если скалярное произведение g невырожденно на V (т.е. $\operatorname{Ker} g = \{\Theta\}$), относительно g могут существовать нетривиальные изотропные подпр-ва (например, одномерные).

В евклидовом пр-ве (скалярное произведение g положительно) всякое подпр-во невырожденно и поэтому нетривиальных изотропных подпр-в нет

Лемма

1. Если L невырожденно отн. скалярного произведения g, то
$$V = L \oplus L^{\perp}$$
2. Если L и $L^{\perp}$ невырождены отн скалярного произв. g, то
$$(L^{\perp})^{\perp} = L$$

Доказательство

1. Пусть $x \in L \cap L^{\perp}$. Тогда
$$g(x, y) = 0$$
для всех $y \in L$, т.е. вектор $x \in \operatorname{Ker} \tilde{g}$, где $\tilde{g}$ – сужение скалярного произведения g на подпр-во L.

Т.к. L невырожденно отн. g, то $\operatorname{Ker} \tilde{g} = \{0\}$ и $x = O$.

Таким образом, $L + L^{\perp} = L \oplus L^{\perp}$.

Пусть $e_1, \dots, e_k$ – нек-рый базис подпр-ва L. Дополним его до базиса $e_1, \dots, e_k, e_{k+1}, \dots, e_n$ пр-ва V. Тогда:
$$L^{\perp} = \{ x \in V \mid g(x, e_j), \ j = 1, \dots, k \}$$
или, в координатах
$$\sum_{i=1}^{n} g_{ij} x_i = 0 \qquad j = 1, \dots, k \qquad (*)$$
Ранг этой ОСЛУ равен k, что следует из невырожденности скал произв-ия g на L.

След-но,

$$\dim L^\perp = n-k = n - \dim L$$

т.е.

$$\dim L^\perp + \dim L = n = \dim V$$

Отсюда $V = L \oplus L^\perp$.

2. Ясно, что $L \subset (L^\perp)^\perp$ (непосредственно следует из определения).

Т.к. по условию $L^\perp$ невырожденно, то

$$\dim (L^\perp)^\perp = n - \dim L^\perp$$

поскольку и L невырожденно, то

$$\dim L^\perp = n - \dim L.$$

Значит,

$$\dim (L^\perp)^\perp = \dim L.$$

Поэтому $(L^\perp)^\perp = L$. См. на обороте

Теорема 2

Пусть $\mathrm{char}\, F \neq 2$ и g - скалярное произведение на V.

Тогда в V существует ортогональный базис $e_1, \dots, e_n$ относительно g, т.е.

$$g(e_i, e_j) = 0 \quad \text{при } i \neq j$$

Доказательство

Индукция по $n \geq 1$

Покажем, что существует такой вектор $e \in V$, что $e \neq 0$ и $g(e,e) \neq 0$. Действительно, пусть $g(x,x) = 0$ для всех $x \in V$.

Но в таком случае $g(x,y) = 0$ для всех $x, y \in V$ (см. рассуждения после опр квадратичной функции), т.е. g тождественно нулевое скалярное произведение и утверждение теоремы тривиально.

Положим $L = \langle e \rangle$. Ясно, что L невырожденно относительно g. По лемме п. 1

Замечание Из доказанного следует, в частности, что

$$\dim L + \dim L^{\perp} = \dim V.$$

Это равенство будет выполняться для любого подпространства L, но при условии невырожденности скалярного произведения на всём пространстве V (ранг системы (*) по-прежнему будет равен k, так как иначе первые k столбцов матрицы (g_{ij}) оказались бы линейно зависимыми). При том же условии будет справедливым и соотношение $(L^{\perp})^{\perp} = L$ (при любом L).

См. стр. 12 в книге: Артин Э. Геометрическая алгебра. М.: Наука, 1969.

имеем

$$V = L \oplus L^{\perp} = \langle e \rangle \oplus V'$$

где $\dim V' = n-1$

К подпр-ву V' применимо предположение индукции, т.е. в нем есть ортогональный базис

Выбрав в V' ортогональный базис и добавив к нему вектор e получим ортогональный базис.

Q: Как практически находить ортогональный базис?

A В евклидовом случае можно применить к произвольному базису процесс ортогонализации Грама-Шмидта. Иначе:

Пусть $e_1, \ldots, e_n$ – базис V, причем все подпр-ва $L_m = \langle e_1, \ldots, e_m \rangle$ $(m = 1, \ldots, n)$ являются невырожденными относительно скалярного произведения g.

Будем искать ортогональный базис $e_1', \ldots, e_n'$ в „треугольном" виде

$$e_1' = t_{11} e_1$$

$$e_2' = t_{12} e_1 + t_{22} e_2$$

$$\ldots$$

$$e_n' = t_{1n} e_1 + t_{2n} e_2 + \ldots + t_{nn} e_n$$

Положим $t_{11} = \frac{1}{g_{11}} = \frac{1}{g(e_1, e_1)}$ и пусть $e_1', \ldots, e_{m-1}'$ уже найдены.

Требуется найти e_m', исходя из условия

$$g(e_m', e_j') = 0 \quad (j = 1, \ldots, m-1) \quad (*)$$

Если потребовать, чтобы выполнялось условие

$$g(e_m', e_j) = 0 \quad (j = 1, \ldots, m-1)$$

то условие $(*)$ также будет выполнено

Имеем:

$$\sum_{i=1}^{m} t_{im} g_{ij} = 0 \quad (j = 1, \ldots, m-1)$$

Добавим еще одно условие:

$$g(e'_m, e_m) = 1$$

и уравнение

$$\sum_{i=1}^{m} t_{im} g_{im} = 1$$

Полученная СЛУ с неизвестными $t_{1m}, t_{2m}, \ldots, t_{mm}$ имеет единственное решение, т.к. по предположению L_m невырожденно, а значит

$$\Delta_m = \det (g_{ij})_{i,j=1}^{m} \neq 0$$

Легко видеть, что

$$t_m = \frac{\Delta_{m-1}}{\Delta_m} \quad \boxed{g(e'_m, e'_m) = g(e'_m, t_{1m}e_1 + \ldots + t_{mm}e_m) = t_m = \frac{\Delta_{m-1}}{\Delta_m}}$$

В рез-те получим базис $e'_1, \ldots, e'_n$, в к-ром матрица Грама скалярного произведения g имеет вид:

$$G' = \begin{pmatrix} \Delta_0/\Delta_1 & & 0 \\ & \ddots & \\ 0 & & \Delta_{n-1}/\Delta_n \end{pmatrix}, \quad \Delta_0 = 1$$

Таким образом, при сделанных предположениях билинейная форма

$$g(x, y) = \sum_{i,j=1}^{n} g_{ij} x_i y_j$$

может быть приведена к виду

$$g(x, y) = \sum_{i=1}^{n} \frac{\Delta_{i-1}}{\Delta_i} x'_i y'_i$$

при помощи треугольного преобразования с матрицей T

$$G' = T^t G T, \text{ где}$$

$$T = \begin{pmatrix} t_{11} & t_{12} & \ldots & t_{1n} \\ 0 & t_{22} & \ldots & t_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & t_{nn} \end{pmatrix}.$$

Этот рез-тат, сформулированный в терминах квадратичной формы носит название теоремы Якоби

Теорема 3 (Якоби)

Если $\Delta_1 \neq 0, \dots, \Delta_n \neq 0$, то квадратичная форма

$$q(x) = \sum_{i,j=1}^{n} g_{ij} x_i x_j$$

$$\Delta_m = \det (g_{ij})_{i,j=1}^{m}$$

треугольным невырожденным преобразованием приводится к виду

$$q(x) = \sum_{m=1}^{n} \frac{\Delta_{m-1}}{\Delta_m} (x'_m)^2$$

В общем случае можно применить метод Лагранжа (метод выделения полного квадрата). Считаем, что $\operatorname{char} F \neq 2$.

Пусть дана квадратичная форма

$$q(x) = \sum_{i,j=1}^{n} g_{ij} x_i x_j$$

Возможны 2 ситуации:

1. Существует ненулевой диагональный эл-нт

Пусть, например, $g_{11} \neq 0$. Имеем:

$$q(x) = g_{11} x_1^2 + x_1 (2 g_{12} x_2 + \dots + 2 g_{1n} x_n) + q'(x_2, \dots, x_n) = g_{11} \left(x_1 + \frac{g_{12}}{g_{11}} x_2 + \dots + \frac{g_{1n}}{g_{11}} x_n\right)^2 + q''(x_2, \dots, x_n)$$

где q', q'' – квадратичные формы от переменных $x_2, \dots, x_n$

Полагая

$$y_1 = x_1 + \frac{g_{12}}{g_{11}} x_2 + \dots + \frac{g_{1n}}{g_{11}} x_n$$

$$y_2 = x_2, \dots, y_n = x_n$$

получим:

$$q(x) = g_{11}y_1^2 + q''(y_2, \dots, y_n)$$

2. Все диагональные эл-ты равны нулю

Можно считать, что $g_{12} \neq 0$. Имеем:

$$q(x) = 2g_{12}x_1x_2 + x_1 l_1(x_3, \dots, x_n) + $$
$$+ x_2 l_2(x_3, \dots, n)$$

где l_1, l_2 – линейные формы относительно указанных переменных.

После замены

$$x_1 = y_1 + y_2 \qquad x_3 = y_3 \qquad \dots \qquad x_{n-1} = y_{n-1}$$
$$x_2 = y_1 - y_2 \qquad x_4 = y_4 \qquad \qquad x_n = y_n$$

будем иметь

$$q(x) = 2g_{12}(y_1^2 - y_2^2) + q'(y_1, y_2, \dots, y_n)$$

где квадратичная форма q' не содержит ни y_1^2, ни y_2^2.

Таким образом, в новых переменных $y_1, y_2, \dots, y_n$ имеем ситуацию п. 1

1.17 17. Линейный оператор в векторном пространстве. Матрица линейного оператора в данном базисе и её изменение при переходе к другому базису.

2. $V_n = \{ f(x) \in \mathbb{R}[x] \mid \deg f(x) \le n \}$

(если $f(x) = a_0 + a_1 x + \ldots + a_n x^n$, $a_n \ne 0$, то $\deg f(x) = n$)

V_n изоморфно $V' = \mathbb{R}^{n+1}$. Здесь $\varphi(a_0 + a_1 x + \ldots + a_n x^n) = (a_0, a_1, \ldots, a_n)$

3 Координаты вектора в базисе

Пусть V – нек-рое n-мерное векторное пространство над полем F.

Опр. Координатами вектора $a \in V$ в базисе $b_1, \ldots, b_n$ называются коэффициенты в разложении

$$a = k_1 b_1 + \ldots + k_n b_n$$

При фиксированном базисе каждому вектору $a \in V$ однозначно сопоставляется набор координат, к-рые записываются в виде столбца

$$a \to \begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix} = (k_1, \ldots, k_n)^t$$

Это сопоставление согласовано с операциями над векторами: при сложении векторов их столбцы складываются, а при умножении вектора на скаляр столбец координат умножается на скаляр.

Пример

Рассмотрим $\mathbb{R}^n$, где в кач-ве базиса взят стандартный базис (базис из единичных векторов).

$e_1 = (1, 0, \ldots, 0)$

$e_2 = (0, 1, \ldots, 0)$

$\ldots$

$e_n = (0, 0, \ldots, 1)$

Тогда столбец координат произвольного вектора

$a = (a_1, \ldots, a_n)$

есть $\begin{pmatrix} a_1 \\ a_n \end{pmatrix}$

Пусть $n=3$. Выберем в $\mathbb{R}^3$ след. базис:

$b_1=(1,1,0)$

$b_2=(0,1,1)$

$b_3=(0,0,1)$

Найдем координаты вектора

$a=(1,2,3)$

в данном базисе.

Имеем:

$$a=k_1b_1+k_2b_2+k_3b_3$$

т.е.

$$(1,2,3)=k_1(1,1,0)+k_2(0,1,1)+k_3(0,0,1)$$

$$\begin{cases} k_1=1 \\ k_1+k_2=2 \\ k_2+k_3=3 \end{cases} \Rightarrow \begin{pmatrix} k_1 \\ k_2 \\ k_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}$$

<u>Замечание</u>

Столбец координат вектора зависит от выбора базиса.

<u>Опр.</u> Пусть $B: b_1,\dots,b_n$ и $B': b_1', b_2', \dots, b_n'$ — 2 базиса n-мерного пр-ва V.

Матрицей перехода от базиса B к базису B' называется такая матрица, столбцы к-рой суть столбцы координат вектора B' в базисе B

Если

$$b_1'=t_{11}b_1+\dots+t_{n1}b_n,$$

$$b_2'=t_{12}b_1+\dots+t_{n2}b_n,$$

$$\dots$$

$$b_n'=t_{n2}b_1+\dots+t_{nn}b_n$$

то

$$T = \begin{pmatrix} t_{11} & \dots & t_{1n} \\ \dots & \dots & \dots \\ t_{n1} & \dots & t_{nn} \end{pmatrix}$$

матрица перехода от B к B' (от старого к новому).

Положим

$$B = (b_1, \dots, b_n)$$

$$B' = (b_1', \dots, b_n')$$

Тогда матрица перехода T может быть определена следующим матричным равенством:

$$B' = B\ T$$

<u>Теорема 16</u>

Всякая матрица перехода является обратимой матрицей.

Любая обратимая матрица может служить матрицей перехода от нек-рого базиса к нек-рому другому базису.

<u>Доказательство</u>

1. Пусть T – матрица перехода от B к B'. Покажем, что T обратима.

Пусть T' – матрица перехода от B' к B. Имеем:

$$B' = B \cdot T \qquad B = B' \cdot T'$$

След-но

$$B = (BT) \cdot T' = B(T\ T')$$

Из теоремы 9 следует, что $T\ T' = E$

Аналогично можно получить рав-во $T' T = E$

Отсюда $T' = T^{-1}$ по определению обратной матрицы.

2. Пусть $B: b_1, \dots, b_n$ нек-рый базис и T – произвольная обратимая матрица квадратная порядка n.

Определим новую систему векторов B' рав-вом

$$B' = B \cdot T$$

Покажем, что B': $b_1', b_2', \dots, b_n'$ является базисом V.

~~Для~~ Для этого достаточно показать, что векторы $b_1', \dots, b_n'$ линейно независимы.

Пусть $b_1', \dots, b_n'$ линейно зависимы. Тогда линейно зависимыми будут столбцы матрицы T:

$$b_1' = t_{11} b_1 + \dots + t_{n1} b_n$$

$$b_2' = t_{12} b_1 + \dots + t_{n2} b_n$$

$$\dots$$

$$b_n' = t_{1n} b_1 + \dots + t_{nn} b_n$$

$$0 = k_1 b_1' + \dots + k_n b_n' = k_1 t_{11} b_1 + \dots + k_1 t_{n1} b_n +$$
$$+ \dots + k_n t_{1n} b_1 + \dots + k_n t_{nn} b_n =$$
$$= (k_1 t_{11} + \dots + k_n t_{1n}) b_1 + \dots + (k_1 t_{n1} + \dots + k_n t_{nn}) b_n$$

$$\begin{cases} k_1 t_{11} + \dots + k_n t_{1n} = 0, \\ \dots \\ k_1 t_{n1} + \dots + k_n t_{nn} = 0. \end{cases}$$

Это рав-во означает, что линейная комбинация столбцов матрицы T с коэффициентами $k_1, \dots, k_n$ есть нулевой вектор, причем из $k_1, \dots, k_n$ не все равны нулю, т.е столбцы T линейно зависимы, однако по условию T обратима, т.е. ее ранг ~~равен~~ полон и она не может иметь линейно зависимые столбцы.

Теорема 17

Пусть B и B' — базисы n-мерного пр-ва V, и к-рые столбцы координат вектора $a \in V$ суть

$$\begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix} \text{ и } \begin{pmatrix} k_1' \\ \vdots \\ k_n' \end{pmatrix}$$

1.18 18. Ядро и образ линейного отображения. Невырожденные линейные операторы.

Определим новую систему векторов B' рав-вом

$$B' = B \cdot T$$

Покажем, что B': $b_1', b_2', \ldots, b_n'$ является базисом V.

Для этого достаточно показать, что векторы $b_1', \ldots, b_n'$ линейно независимы.

Пусть $b_1', \ldots, b_n'$ линейно зависимы. Тогда линейно зависимыми будут столбцы матрицы T:

$$b_1' = t_{11} b_1 + \ldots + t_{n1} b_n$$

$$b_2' = t_{12} b_1 + \ldots + t_{n2} b_n$$

$$\ldots$$

$$b_n' = t_{1n} b_1 + \ldots + t_{nn} b_n$$

$$0 = k_1 b_1' + \ldots + k_n b_n' = k_1 t_{11} b_1 + \ldots + k_1 t_{n1} b_n + $$
$$+ \ldots + k_n t_{1n} b_1 + \ldots + k_n t_{nn} b_n =$$
$$= (k_1 t_{11} + \ldots + k_n t_{1n}) b_1 + \ldots + (k_1 t_{n1} + \ldots + k_n t_{nn}) b_n$$

$$\begin{cases} k_1 t_{11} + \ldots + k_n t_{1n} = 0, \\ \ldots \\ k_1 t_{n1} + \ldots + k_n t_{nn} = 0. \end{cases}$$

Это рав-во означает, что линейная комбинация столбцов матрицы T с коэффициентами $k_1, \ldots, k_n$ есть нулевой вектор, причем из $k_1, \ldots, k_n$ не все равны нулю, т.е столбцы T линейно зависимы, однако по условию T обратима, т.е. ее ранг ~~равен~~ полон и она не может иметь линейно зависимые столбцы.

Теорема 17

Пусть B и B' — базисы n-мерного пр-ва V, и к-рые столбцы координат вектора $a \in V$ суть

$$\begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix} \text{ и } \begin{pmatrix} k_1' \\ \vdots \\ k_n' \end{pmatrix}$$

Тогда:

$$\begin{pmatrix} k_1 \\ \dots \\ k_n \end{pmatrix} = T \begin{pmatrix} k_1' \\ \dots \\ k_n' \end{pmatrix}$$

где T – матрица перехода от B к B'.

Доказательство

Имеем $B' = BT$, $a = k_1 b_1 + \dots + k_n b_n = k_1' b_1' + \dots + k_n' b_n'$

Другими словами,

$$B \begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix} = B' \begin{pmatrix} k_1' \\ \vdots \\ k_n' \end{pmatrix}$$

Отсюда

$$B \begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix} = (BT) \begin{pmatrix} k_1' \\ \dots \\ k_n' \end{pmatrix} = B \left(T \begin{pmatrix} k_1' \\ \dots \\ k_n' \end{pmatrix} \right).$$

След-но:

$$\begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix} = T \begin{pmatrix} k_1' \\ \dots \\ k_n' \end{pmatrix}$$

Замечание

Обычно используют эквивалентный вариант полученной формулы:

$$\begin{pmatrix} k_1' \\ \dots \\ k_n' \end{pmatrix} = T^{-1} \begin{pmatrix} k_1 \\ \dots \\ k_n \end{pmatrix}$$

Пример

$V = \mathbb{R}^3$, $B = e_1, e_2, e_3$ (станд. базис)

B': $e_1' = (5, -1, -2)$,

$e_2' = (2, 3, 0)$,

$e_3' = (-2, 1, 1)$.

Имеем:

(119)

$$T = \begin{pmatrix} 5 & 2 & -2 \\ -1 & 3 & 1 \\ -2 & 0 & 1 \end{pmatrix}$$

Эта матрица обратима и

$$T^{-1} = \begin{pmatrix} 3 & -2 & 8 \\ -1 & 1 & -3 \\ 6 & -4 & 17 \end{pmatrix}$$

Пусть $a = (1, 4, -1)$

Найдем координаты вектора a в базисе B':

$$\begin{pmatrix} k_1' \\ k_2' \\ k_3' \end{pmatrix} = \begin{pmatrix} 3 & -2 & 8 \\ -1 & 1 & -3 \\ 6 & -4 & 17 \end{pmatrix} \begin{pmatrix} 1 \\ 4 \\ -1 \end{pmatrix} = \begin{pmatrix} -13 \\ 6 \\ -27 \end{pmatrix}$$

п. 3 Сигнатура скалярного произведения

В этом пункте считаем $F = \mathbb{R}$.

Пусть $e_1, .., e_n$ — нек-рый ортогональный базис V, в к-ром задано скалярное произведение g.

Опр. Сигнатурой скалярного произведения g в ортогональном базисе $e_1, ..., e_n$ наз. тройка

(r, s, t). $\quad g(e_1, e_1), g(e_2, e_2), .., g(e_n, e_n)$

где r — число „положительных квадратов",
s — число „отрицательных квадратов",
t — число „нулевых квадратов"

Теорема 4 (закон инерции)

Сигнатура (r, s, t) не зависит от выбора ортогонального базиса отн. скалярного пр g.

<u>Доказательство</u>

Т.к. $r+s=\operatorname{rank}(g)$ – инвариант, то число $t=n-(r+s)$ не зависит от выбора ортогонального базиса.

Пусть $L_0=\operatorname{Ker} g$, Тогда:

$$V=L_0\oplus L_+\oplus L_-=L_0\oplus L'_+\oplus L'_-$$

Здесь $L_+, L_-; L'_+, L'_-$ – подпр-ва, соотв положительным и отрицательным диагональным эл-там матрицы Грама двух различных ортогональных базисов.

Нужно док-ть, что $\dim L_+=\dim L'_+$ и $\dim L_-=\dim L'_-$.

Рассуждая от противного, предположим, что

$$r=\dim L_+ > r'=\dim L'_+$$

Пусть $a_1,\dots,a_r$ – нек-рый базис подпр-ва L_+. Тогда

$$a_i=b_i+c_i+d_i \quad (i=1,\dots,r)$$

где $b_i\in L_0$, $c_i\in L'_+$, $d_i\in L'_-$.

Векторы $c_1,\dots,c_r$ линейно зависимы, т.к. по предположению $r'<r$, т.е.

$$k_1c_1+\dots+k_rc_r=0$$

для нек-рых k_i, среди к-рых есть отличные от нуля.

Отсюда получаем

$$a=b+d$$

где $a=\sum_{i=1}^{r}k_ia_i$, $b=\sum_{i=1}^{r}k_ib_i$, $d=\sum_{i=1}^{r}k_id_i$

При этом $a\neq 0$, т.к $a_i\neq 0$ $(i=1,\dots,r)$ как базисные, среди k_i есть ненулевой.

Полученное рав-во противоречиво, т.к.

$$\underset{a\in L_+,\,a\neq 0}{0<} g(a,a)=\underbrace{g(b,b)}_{=0}+2\underbrace{g(b,d)}_{=0}+g(d,d)=g(d,d)\underset{\text{т.к. } d\in L_-}{\leq 0}$$

т.к. $b\in L_0$

След-но $r=r'$, а значит и $t=t'$.

Обычно закон инерции формулируют в терминах квадратичных форм: если квадратичную форму

$$q(x) = \sum_{i=1}^{n} g_{ij} x_i x_j$$

привести к сумме квадратов

$$\lambda_1 (x_1')^2 + \dots + \lambda_n (x_n')^2$$

то число положительных, отрицательных, равных нулю коэффициентов не зависит от способов приведения.

Если матрица квадр. формы $G = (g_{ij})_{i,j=1}^{n}$ такова, что

$$\Delta_1 \neq 0, \dots, \Delta_n \neq 0$$

т.е. все ее главные миноры отличны от нуля, то число отрицательных коэффициентов равно числу перемен знака в числовой послед-ти

$$1, \Delta_1, \Delta_2, \dots, \Delta_{n-1}, \Delta_n$$

(следствие теоремы Якоби).

Справедлива также след. теорема:

<u>Теорема 5.</u> (критерий Сильвестра)

Квадратичная форма

$$q(x) = \sum_{i,j=1}^{n} g_{ij} x_i x_j$$

является положительно определенной, (т.е. $q(x) > 0$ для всех $x \neq 0$) тогда и только тогда, когда

$$\Delta_1 > 0, \dots, \Delta_n > 0$$

<u>Доказательство</u>. следует из теоремы Якоби.

1.19 19. Собственные значения и собственные векторы линейного оператора. Характеристический многочлен линейного оператора.

§ 2. ПОДПРОСТРАНСТВА ВЕКТОРНОГО ПРОСТРАНСТВА

Подпространство. Пусть $\mathcal{V}$ — векторное пространство над полем $\mathcal{F}$ и $U \subset V$. Множество U называется *замкнутым* в $\mathcal{V}$, если оно замкнуто относительно главных операций $\mathcal{V}$, операций сложения и умножения на скаляры, т. е. для любых $\boldsymbol{a}$, $\boldsymbol{b}$ из U и любого λ из F $\boldsymbol{a}+\boldsymbol{b} \in U$ и $\lambda\boldsymbol{a} \in U$.

ОПРЕДЕЛЕНИЕ. *Подпространством векторного пространства* $\mathcal{V}$ называется любая подалгебра пространства $\mathcal{V}$, рассматриваемого как алгебра.

Пусть $\mathcal{V} = \langle V, +, \{\omega_\lambda \mid \lambda \in F\}\rangle$ — векторное пространство над $\mathcal{F}$. Пусть $\mathcal{U}$ — подалгебра пространства $\mathcal{V}$ и U — его основное множество. Тогда U — непустое подмножество множества V, замкнутое в $\mathcal{V}$. Пусть $\oplus$ и ω'_λ — ограничения главных операций «$+$» и ω_λ пространства $\mathcal{V}$ множеством U, т. е.

$$\boldsymbol{a} \oplus \boldsymbol{b} = \boldsymbol{a} + \boldsymbol{b} \text{ для любых } \boldsymbol{a}, \boldsymbol{b} \text{ из } U,$$

$$\omega'_\lambda \boldsymbol{a} = \omega_\lambda \boldsymbol{a} = \lambda \boldsymbol{a} \text{ для любого } \boldsymbol{a} \text{ из } U;$$

тогда

(1) $\mathcal{U} = \langle U, \oplus, \{\omega'_\lambda \mid \lambda \in F\}\rangle$.

Однако вместо записи (1) обычно пишут

$$\mathcal{U} = \langle U, +, \{\omega_\lambda \mid \lambda \in F\}\rangle.$$

Отметим следующие свойства подпространств.

СВОЙСТВО 2.1. *Если $\mathcal{V}$ — векторное пространство над полем $\mathcal{F}$, то любое его подпространство является векторным пространством над $\mathcal{F}$.*

СВОЙСТВО 2.2. *Если $\mathcal{W}$ — подпространство векторного пространства $\mathcal{U}$ и $\mathcal{U}$ — подпространство векторного пространства $\mathcal{V}$, то $\mathcal{W}$ является подпространством пространства $\mathcal{V}$.*

Пересечением подпространств $\mathcal{U}_1, \ldots, \mathcal{U}_m$ векторного пространства $\mathcal{V}$ называется подпространство $\mathcal{V}$ с основным множеством $U_1 \cap U_2 \cap, \ldots, \cap U_m$. Аналогично определится пересечение бесконечного множества подпространств пространства $\mathcal{V}$.

СВОЙСТВО 2.3. *Пересечение любого множества подпространств векторного пространства $\mathcal{V}$ является подпространством пространства $\mathcal{V}$.*

Свойства 2.2 и 2.3 следуют из теорем 3.1.7 и 3.1.9 соответственно.

Линейная оболочка множества векторов. Пусть $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n\}$ — конечное множество векторов векторного пространства $\mathscr{V}$. Вектор $\lambda_1 \boldsymbol{a}_1+\ldots+\lambda_n \boldsymbol{a}_n$ называется *линейной комбинацией векторов* $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ с коэффициентами из F.

ОПРЕДЕЛЕНИЕ. Множество $\{\lambda_1 \boldsymbol{a}_1+\ldots+\lambda_n \boldsymbol{a}_n \mid \lambda_1, \ldots, \lambda_n \in F\}$ всех линейных комбинаций векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ с коэффициентами из F называется *линейной оболочкой векторов* $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ и обозначается через $L(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$.

Легко видеть, что линейная оболочка векторов замкнута в $\mathscr{V}$, т. е. замкнута относительно всех главных операций пространства $\mathscr{V}$ (сложения и умножений на скаляры).

ОПРЕДЕЛЕНИЕ. Подпространство векторного пространства $\mathscr{V}$ с основным множеством $L(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$ обозначается через $\mathscr{L}(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$ и называется *подпространством*, натянутым на векторы $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$, или подпространством, порожденным векторами $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$.

ОПРЕДЕЛЕНИЕ. *Линейной оболочкой множества* M, $M \subset V$, называется совокупность $L(M)$ всех линейных комбинаций векторов из M с коэффициентами из F. *Линейной оболочкой пустого множества* называется множество $\{\boldsymbol{0}\}$.

Линейная оболочка множества M замкнута в $\mathscr{V}$.

ОПРЕДЕЛЕНИЕ. Подпространство пространства $\mathscr{V}$ с основным множеством $L(M)$ обозначается через $\mathscr{L}(M)$ и называется *подпространством, натянутым на множество* M, или *подпространством, порожденным множеством* M.

Сумма подпространств. Пусть $\mathscr{U}_1, \ldots, \mathscr{U}_m$ — подпространства векторного пространства $\mathscr{V}$ и $U_1, \ldots, U_m$ — их основные множества. Множество

$$\{\boldsymbol{a}_1+\ldots+\boldsymbol{a}_m \mid \boldsymbol{a}_1 \in U_1, \ \ldots, \ \boldsymbol{a}_m \in U_m\}$$

обозначается через $U_1+\ldots+U_m$. Легко проверить, что это множество замкнуто в пространстве $\mathscr{V}$.

ОПРЕДЕЛЕНИЕ. Подпространство пространства $\mathscr{V}$ с основным множеством $U_1+\ldots+U_m$ называется *суммой подпространств* $\mathscr{U}_1, \ldots, \mathscr{U}_m$ и обозначается через $\mathscr{U}_1+\ldots+\mathscr{U}_m$.

Отметим следующие свойства суммы подпространств, легко вытекающие из ее определения.

СВОЙСТВО 2.4. Если $\mathscr{L}$ и $\mathscr{U}$ — подпространства векторного пространства $\mathscr{V}$, то $\mathscr{U}+\mathscr{L}=\mathscr{L}+\mathscr{U}$.

СВОЙСТВО 2.5. Если $\mathscr{L}, \mathscr{U}, \mathscr{W}$ — подпространства векторного пространства $\mathscr{V}$, то $\mathscr{L}+(\mathscr{U}+\mathscr{W})=(\mathscr{L}+\mathscr{U})+\mathscr{W}$.

СВОЙСТВО 2.6. Если $\mathscr{L}$ — подпространство пространства $\mathscr{U}$, то $\mathscr{L}+\mathscr{U}=\mathscr{U}$.

Пусть $\mathscr{L}_1, \ldots, \mathscr{L}_m$ — подпространства векторного пространства $\mathscr{V}$.

ОПРЕДЕЛЕНИЕ. Сумма $\mathscr{L}_1+\ldots+\mathscr{L}_m$ называется *прямой суммой подпространств* $\mathscr{L}_1, \ldots, \mathscr{L}_m$ и обозначается через $\mathscr{L}_1 \oplus \ldots \oplus \mathscr{L}_m$, если любой вектор $\boldsymbol{a}$ из $L_1+\ldots+L_m$ можно единственным образом представить в виде

$$\boldsymbol{a}=\boldsymbol{a}_1+\ldots+\boldsymbol{a}_m, \text{ где } \boldsymbol{a}_1 \in L_1, \ldots, \boldsymbol{a}_m \in L_m.$$

Другими словами, сумма $\mathscr{L}_1+\ldots+\mathscr{L}_m$ называется *прямой*, если для любых $\boldsymbol{a}_1, \boldsymbol{b}_1$ из $L_1, \ldots, \boldsymbol{a}_m, \boldsymbol{b}_m$ из L_m равенство $\boldsymbol{a}_1+\ldots+\boldsymbol{a}_m=\boldsymbol{b}_1+\ldots+\boldsymbol{b}_m$ влечет равенства $\boldsymbol{a}_1=\boldsymbol{b}_1, \ldots, \boldsymbol{a}_m=\boldsymbol{b}_m$.

ТЕОРЕМА 2.1. *Сумма подпространств $\mathscr{L}$ и $\mathscr{U}$ векторного пространства является прямой тогда и только тогда, когда $L \cap U=\{\mathbf{0}\}$.*

Доказательство. Предположим, что $\mathscr{L}+\mathscr{U}=\mathscr{L}\oplus\mathscr{U}$. Тогда для любого элемента $\boldsymbol{c}$ из $L \cap U$ верно равенство $\boldsymbol{c}+\mathbf{0}=\mathbf{0}+\boldsymbol{c}$, из которого следует равенство $\boldsymbol{c}=\mathbf{0}$, так как сумма $\mathscr{L}+\mathscr{U}$ прямая. Следовательно, $L \cap U=\{\mathbf{0}\}$.

Предположим теперь, что $L \cap U=\{\mathbf{0}\}$. Для любых векторов $\boldsymbol{a}_1$, $\boldsymbol{b}_1$ из L и $\boldsymbol{a}_2$, $\boldsymbol{b}_2$ из U равенство $\boldsymbol{a}_1+\boldsymbol{a}_2=\boldsymbol{b}_1+\boldsymbol{b}_2$ влечет соотношения $\boldsymbol{a}_1-\boldsymbol{b}_1=\boldsymbol{a}_2-\boldsymbol{b}_2 \in L \cap U=\{\mathbf{0}\}$, поэтому $\boldsymbol{a}_1=\boldsymbol{b}_1$ и $\boldsymbol{a}_2=\boldsymbol{b}_2$. Следовательно, сумма $\mathscr{L}+\mathscr{U}$ является прямой. □

ТЕОРЕМА 2.2. *Сумма подпространств $\mathscr{L}_1, \ldots, \mathscr{L}_m$ векторного пространства является прямой суммой, если для любых векторов $\boldsymbol{a}_1$ из $L_1, \ldots, \boldsymbol{a}_m$ из L_m равенство*

(1) $\boldsymbol{a}_1+\ldots+\boldsymbol{a}_m=\mathbf{0}$

влечет равенства

(2) $\boldsymbol{a}_1=\mathbf{0}, \ldots, \boldsymbol{a}_m=\mathbf{0}$.

Доказательство. Предположим, что сумма $\mathscr{L}_1+\ldots+\mathscr{L}_m$ прямая. Тогда из равенства (1), которое можно записать в виде $\boldsymbol{a}_1+\ldots+\boldsymbol{a}_m=\mathbf{0}+\ldots+\mathbf{0}$, следуют равенства $\boldsymbol{a}_1=\mathbf{0}, \ldots, \boldsymbol{a}_m=\mathbf{0}$.

Предположим теперь, что для любых векторов $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ соответственно из $L_1, \ldots, L_m$ равенство (1) влечет равенства (2). Каковы бы ни были векторы $\boldsymbol{b}_1$, $\boldsymbol{c}_1$ из $L_1, \ldots, \boldsymbol{b}_m$, $\boldsymbol{c}_m$ из L_m, равенство

(3) $\boldsymbol{b}_1+\ldots+\boldsymbol{b}_m=\boldsymbol{c}_1+\ldots+\boldsymbol{c}_m$

влечет $(\boldsymbol{b}_1-\boldsymbol{c}_1)+\ldots+(\boldsymbol{b}_m-\boldsymbol{c}_m)=0$, из которого, по условию, следуют равенства

$$\boldsymbol{b}_1-\boldsymbol{c}_1=0,\ \ldots,\ \boldsymbol{b}_m-\boldsymbol{c}_m=\mathbf{0}.$$

Таким образом, из (3) следуют равенства

$$\boldsymbol{b}_1=\boldsymbol{c}_1,\ \ldots,\ \boldsymbol{b}_m=\boldsymbol{c}_m.$$

Следовательно, сумма $\mathscr{L}_1+\ldots+\mathscr{L}_m$ является прямой. □

Линейные многообразия. Пусть $\mathscr{L}$ — подпространство векторного пространства $\mathscr{V}$ и L — его основное множество. На множестве V определим бинарное отношение $\sim$, считая, что $a\sim b$ тогда и только тогда, когда $\boldsymbol{a}-\boldsymbol{b}\in L$. Назовем это бинарное отношение *отношением сравнения по* $\mathscr{L}$.

ПРЕДЛОЖЕНИЕ 2.3. *Отношение сравнения на множестве V по $\mathscr{L}$ является отношением эквивалентности на V.*

Доказательство. Отношение сравнения по $\mathscr{L}$, очевидно, рефлексивно. Отношение по $\mathscr{L}$ симметрично, так как из $\boldsymbol{a}-\boldsymbol{b}\in L$ следует $\boldsymbol{b}-\boldsymbol{a}\in L$. Отношение сравнения по $\mathscr{L}$ транзитивно, так как для любых $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}\in V$ из $\boldsymbol{a}-\boldsymbol{b}\in L$ и $\boldsymbol{b}-\boldsymbol{c}\in L$ следует, что $\boldsymbol{a}-\boldsymbol{c}=(\boldsymbol{a}-\boldsymbol{b})+(\boldsymbol{b}-\boldsymbol{c})\in L$. Следовательно, отношение сравнения по $\mathscr{L}$ является отношением эквивалентности на множестве V. □

Отношение эквивалентности $\sim$ на V определяет разбиение множества V на классы эквивалентности.

ОПРЕДЕЛЕНИЕ. Пусть $\mathscr{L}$ — подпространство векторного пространства $\mathscr{V}$. Любой класс эквивалентности отношения сравнения по $\mathscr{L}$ называется *линейным многообразием пространства $\mathscr{V}$ с направлением $\mathscr{L}$.*

Пример. Множество всех решений совместной системы линейных уравнений с n переменными является линейным многообразием с направлением $\mathscr{L}$ n-мерного арифметического векторного пространства, где $\mathscr{L}$ — пространство решений соответствующей однородной системы уравнений.

Из приведенного выше определения вытекают свойства 2.7 и 2.8.

СВОЙСТВО 2.7. *Два вектора векторного пространства $\mathscr{V}$ принадлежат одному и тому же линейному многообразию с направлением $\mathscr{L}$ тогда и только тогда, когда их разность принадлежит L.*

СВОЙСТВО 2.8. *Любые два линейных многообразия векторного пространства $\mathscr{V}$ с направлением $\mathscr{L}$ либо совпадают, либо не пересекаются. Объединение всех линейных*

п. 4 Приведение к главным осям

Как и в предыдущем пункте, считаем $F = \mathbb{R}$

Пусть V — евклидово пр-во, скалярное произведение в к-ром обозначим $g(x, y)$

Предположим, что на V задана нек-рая произвол. билинейная ф-ия g при помощи матрицы

Грама $G = (g_{ij})$, где $g_{ij} = g(e_i, e_j)$, $e_1, \ldots, e_n$ — ортонормированный относительно скалярного произведения (x, y) базис V.

<u>Теорема 6</u> (о приведении к главным осям)

Существует ортонормированный базис $e_1', \ldots, e_n'$ евклидова пр-ва V, в к-ром матрица Грама G скалярного произведения g является диагональной.

Иными словами, после нек-рого ортогонального преобразования квадратичная ф-ия

$$q(x) = g(x, x)$$

может быть записана в виде

$$q(x) = \lambda_1 (x_1')^2 + \ldots + \lambda_n (x_n')^2$$

т.е, как говорят, приведена к главным осям.

<u>Доказательство</u>

Зададим в евклидовом пр-ве V самосопряж. оператор $\varphi: V \to V$ при помощи матрицы G в базисе $e_1, \ldots, e_n$

Поскольку базис $e_1, \ldots, e_n$ — ортонормированный, а матрица G симметрична, так заданный оператор φ будет самосопряженным

Легко видеть, что

$$q(x) = (\varphi(x), x)$$

для всех $x \in V$ (проверяется непосредственным вычислением в координатах относительно базиса $e_1, \ldots, e_n$)

Согласно Теореме 10 § 14 в нек-ром ортонормированном базисе $e_1', \ldots, e_n'$ матрица оператора φ будет диагональной:

$$A'_\varphi = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

Напомним, что $A_\varphi = G$. Имеем:

$$(\varphi(x), x) = (\varphi(x_1' e_1' + \ldots + x_n' e_n'), x_1' e_1' + \ldots + x_n' e_n') =$$
$$= (\lambda_1 x_1' e_1' + \ldots + \lambda_n x_n' e_n', x_1' e_1' + \ldots + x_n' e_n') =$$

$= \lambda_1 (x_1')^2 + \ldots + \lambda_n (x_n')^2$

$A'_\varphi = T^{-1} A_\varphi T =$
$= T^t B T$, так как T — ортогональное преобразование (лучше — ортогональная матрица)

След-но, $q(x)$ имеет нужный вид.

Пример

Пусть $V = \mathbb{R}^2$ — евклидово пр-во со стандартным скалярным произв. (x, y)

Положим $q(x) = x_1^2 + x_1 x_2 + x_2^2$, где $x = (x_1, x_2)$

Каков вид кривой $q(x) = 1$?

В координатах: $x_1^2 + x_1 x_2 + x_2^2 = 1$.

Д/ выяснения этого вопроса необходимо следовать док-ву Теоремы 6.

Рассмотрим нек-рое приложение Теоремы 6:

1. Приведение пары квадратичных форм, одна из к-рых положительно определена к сумме квадратов невырожденным преобразованием.

   Пусть V — вещественное векторное пр-во на к-ром заданы 2 квадратичные ф-ии $q_1(x)$ и $q_2(x)$, при этом $q_1(x)$ положительно определена, т.е. $q_1(x) > 0$ д/ всех $x \in V$, $x \neq 0$.

   Требуется найти такое невырожденное преобразование при к-ром квадратичная форма $q_1(x)$ запишется как

   $(x_1')^2 + \ldots + (x_n')^2$

   а квадратичная форма q_2 как

   $\lambda_1 (x_1')^2 + \ldots + \lambda_n (x_n')^2$

   Это возможно сделать на основе Теоремы 6, т.к. в пр-ве V можно ввести евклидову структуру при помощи квадратичной формы $q_1(x)$ (положить $(x, y) = g_1(x, y)$), где g_1 — билинейная ф-ия, полярная к квадратичной ф-ии q_1).

2. Нахождение угла м/у 2-мя подпр-вами в евклидовом пр-ве.

   Пусть V — евклидово пр-во со скалярным произведением (x, y), L_1, L_2 — подпр-ва V.

Будем считать, что $L_1 \cap L_2 = \{0\}$, что не ограничивает общности рассуждений (см. определение угла м/у подпр-вами в п. 3 §11).

По определению угол φ м/у L_1 и L_2 находится по ф-ле

$$\cos\varphi = \max_{\substack{0 \neq a \in L_1 \\ 0 \neq b \in L_2}} \frac{(a, b)}{|a||b|}$$

Задача вычисления этого максимума может быть сведена к задаче одновременного приведения пары квадратичных форм к сумме квадратов, а именно, потребуется решать задачу об отыскании величины вида

$$\max_{0 \neq x \in V} \frac{q_2(x)}{q_1(x)} = M$$

Имеем после соответствующего невырожд. преобразования:

$$M = \max_{0 \neq x \in V} \frac{q_2(x)}{q_1(x)} = \max_{(0, \dots, 0) \neq (x_1', \dots, x_n')} \frac{\lambda_1 (x_1')^2 + \dots + \lambda_n (x_n')^2}{(x_1')^2 + \dots + (x_n')^2} =$$

$$= \max\{\lambda_1, \dots, \lambda_n\}$$

1.20 20. Линейная независимость собственных векторов, принадлежащих попарно различным собственным значениям.

п. 4 Суммы и прямые суммы подпространств

Примером подпространства служит линейная оболочка конечной системы векторов:

$$\langle a_1, \dots, a_n \rangle = \{ k_1 a_1 + \dots + k_n a_n \mid k_i \in F \ (i = 1, \dots, n) \}$$

Опр. Суммой подпространств $L_1, \dots, L_m$ пространства V называется подпространство $L = \{ x_1 + \dots + x_m \mid x_i \in L_i \ (i = 1, \dots, m) \}$

Обозначение

$$L = L_1 + \dots + L_m$$

Замечание

Так определенное мн-во L действительно является подпространством, что легко следует из характеристического признака подпространства

Опр. Сумма $L = L_1 + \dots + L_m$ называется прямой, если всякий вектор $x \in L$ допускает единственное представление в виде $x = x_1 + \dots + x_m$, где $x_i \in L_i$ $(i = 1, \dots, m)$

Обозначение $L = L_1 \oplus \dots \oplus L_m$

Примеры

$V = \mathbb{R}^3$

$L_1 = \{ x \in \mathbb{R}^3 / x_1 + x_2 + x_3 = 0 \}$

$L_2 = \langle (1,1,1) \rangle$

Имеем: $L = L_1 + L_2 = \mathbb{R}^3$

Более того, $\mathbb{R}^3 = L_1 \oplus L_2$

Теорема 18

Если $L_1, .., L_m$ конечномерны, то $L = L_1 + .. + L_m$ также конечномерно.

При этом $\dim L \leq \dim L_1 + . \; + \dim L_m$

Равенство $\dim L = \dim L_1 + \; . + \dim L_m$ имеет место тогда и только тогда, когда $L = L_1 \oplus \ldots \oplus L_m$

Доказательство

Пусть $B_1, .., B_m$ – базисы подпр-в $L_1, ..., L_m$.

Обозначим ч/з B систему векторов, полученную соединением систем векторов $B_1, .., B_m$ (в частности, число векторов в системе B $|B| = |B_1| + .. + |B_m|$, т.е. одинаковые векторы не группируются)

1. Заметим, что $L = L_1 + \ldots + L_m = \langle B_1 \rangle + .. + \langle B_m \rangle = \langle B \rangle$

   Так как размерность $\langle B \rangle$ равна рангу порождающей системы B (в кач-ве базиса линейной оболочки можно взять какой-нибудь базис порождающей системы векторов), а $\operatorname{rank} B \leq |B|$, то

   $$\dim L \leq |B_1| + . \; . + |B_m| = \dim L_1 + \; + \dim L_m$$

2. Равенство возможно тогда и только тогда, когда $\operatorname{rank} B = |B| \Leftrightarrow B$ линейно независимая система $\Leftrightarrow$ $L = L_1 \oplus ... \oplus L_m$

Теорема 19 (критерий прямой суммы)

$L = L_1 \oplus .. \oplus L_m \Leftrightarrow L_i \cap (L_1 + . \; . + L_{i-1} + L_{i+1} + \; L_m) = \{0\}$ для любого $i = 1, ..., m$

Доказательство

$\Rightarrow$ Докажем, например, что

$$L_1 \cap (L_2+\dots+L_m)=\{0\}$$

Пусть $x\in L_1\cap(L_2+\dots+L_m)$. Тогда $x\in L_1$, $x=x_2+\dots+x_m$, где $x_2\in L_2,\dots,x_m\in L_m$

След-но,

$$0=\underset{\in L_1}{(-x)}+\underset{\in L_2}{x_2}+\dots+\underset{\in L_m}{x_m}=0+0\dots+0$$

Т.е. существуют 2 представления нулевого вектора ч/з вектора из $L_1,\dots,L_m$, но при этом L - прямая сумма, след-но эти суммы след-но $-x=0$, $x=0$, что и требовалось док-ть.

$\Leftarrow$ Пусть все пересечения $L_i\cap(L_1+\dots+L_{i-1}+L_{i+1}+\dots+L_m)$ нулевые.

Докажем, что $L=L_1\oplus\dots\oplus L_m$

Пусть $x\in L$ и $x=x_1+\dots+x_m=y_1+\dots+y_m$, где $x_i, y_i\in L_i$ $(i=1,\dots,m)$

Тогда $\underset{\in L_1}{x_1-y_1}=\underset{\in L_2}{(y_2-x_2)}+\dots+\underset{\in L_m}{(y_m-x_m)}\in L_2+\dots+L_m$

Т.е. $x_1-y_1\in L_1\cap(L_2+\dots+L_m)=\{0\}$, след-но $x_1-y_1=0$.

Значит, $x_1=y_1$. Аналогично доказывается, что $x_2=y_2,\dots,x_m=y_m$.

Пример

Сумма $\{x\in\mathbb{R}^3 \mid x_1+x_2+x_3=0\}+\langle(1,1,1)\rangle$ является прямой, т.к. эти подпространства имеют нулевое пересечение

Рассмотрим случай $m=2$

Теорема 20

$$\dim(L_1+L_2)=\dim(L_1)+\dim(L_2)-\dim(L_1\cap L_2)$$

Доказательство

Считаем, что L_1, L_2 конечномерны.

Пусть $b_1, .., b_k$ — базис $L_1 \cap L_2$, $\dim(L_1 \cap L_2) = k$

Дополним линейно независимую систему $b_1, \dots, b_k \in L_1, L_2$ до базиса L_1, L_2

$b_1, \dots, b_k, u_1, \dots, u_l$ $(\dim L_1 = k + l)$

$b_1, \dots, b_k, v_1, \dots, v_m$ $(\dim L_2 = k + m)$

Докажем, что векторы $b_1, \dots, b_k, u_1, \dots, u_l, v_1, \dots, v_m$ образуют базис $L_1 + L_2$ (в таком случае будем иметь $k + l + m = (k+l) + (k+m) - k$)

1. Проверим линейную независимость векторов $b_1, .., b_k, u_1, \dots, u_l, v_1, \dots, v_m$

Пусть $p_1 b_1 + .. + p_k b_k + q_1 u_1 + \dots + q_l u_l + r_1 v_1 + .. + r_m v_m = 0$ (*)

$r_1 v_1 + .. + r_m v_m = b$, $q_1 u_1 + \dots + q_l u_l = u$,
$p_1 b_1 + .. + p_k b_k = b$

$L_2 \ni v = -b - u \in L_1$

Так как $v \in L_1$, $v \in L_2$, то $v \in L_1 \cap L_2$, след-но

$v = s_1 b_1 + \dots + s_k b_k$

и, таким образом,

$(p_1 + s_1) b_1 + \dots + (p_k + s_k) b_k + q_1 u_1 + .. + q_l u_l = 0$

Поскольку векторы $b_1, .., b_k, u_1, \dots, u_l$ линейно независимы, т.к. они образуют базис L_1, то, в частности

$q_1 = \dots = q_l = 0$

Итак, $u = 0$. Аналогично доказывается, что $v = 0$. Отсюда и $b = 0$, т.е. линейная комбинация (*) тривиальна

2. Убедимся, что $\langle b_1, \dots, b_k, u_1, .., u_l, q_1, \dots, q_l \rangle = L_1 + L_2$, т.е. всякий вектор $x \in L_1 + L_2$ представим в виде линейной комбинации указанных векторов

Имеем $x = x_1 + x_2$, где $x_1 \in L_1$, $x_2 \in L_2$

Где x_1, x_2 линейно выражаются ч/з базисы L_1 и L_2 соответственно, т.е.

$$x_1 = r_1 b_1 + \ldots + r_k b_k + s_1 u_1 + \ldots + s_e u_e$$

$$x_2 = p_1 b_1 + \ldots + p_k b_k + q_1 v_1 + \ldots + q_m v_m$$

След-но x линейно выражается ч/з $b_1, \ldots, b_k, u_1, \ldots, u_e, v_1, \ldots, v_m$

п. 5 Фактор пространство

Пусть V - векторное пространство, L - подпр-во V

Опр Вектора $x, y \in V$ назовем L-эквивалентными, если $x - y \in L$ ($x \overset{L}{\sim} y$)

Отношение L-эквивалентности, заданное на мн-ве V, является отношением эквивалентности на этом мн-ве, т.е.

1. $x \overset{L}{\sim} x$ для любого $x \in V$
2. Если $x \overset{L}{\sim} y$, то $y \overset{L}{\sim} x$ $\forall x, y \in V$
3. Если $x \overset{L}{\sim} y$, $y \overset{L}{\sim} z$, то $x \overset{L}{\sim} z$ $\forall x, y, z \in V$

Рассмотрим фактор множество $V/\overset{L}{\sim} = V/L$, элементами к-рого служат классы L-эквивалентных векторов простр-ва V

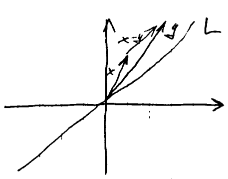
Пример

$V = \mathbb{R}^2$, $L = \langle (1,1) \rangle$

Пусть $x = (x_1, x_2)$, $y = (y_1, y_2)$

$x \overset{L}{\sim} y \Leftrightarrow x - y \in L \Leftrightarrow$

$\Leftrightarrow (x_1 - y_1) - (x_2 - y_2) = 0$



Опр. Множество $x + L = \{x + y \mid y \in L\}$ называется линейным многообразием пр-ва V (здесь x - произвольный вектор из V, L - подпр-во V)

Определим на фактор-мн-ве V/L операции сложения и умножения на скаляр

Пусть $x + L$, $y + L \in V/L$, $k \in F$. Положим:

$(x + L) + (y + L) = (x+y) + L$

$k(x + L) = (kx) + L$

ДГВА

§1. Кольцо многочленов $K[x_1, \ldots, x_n]$

Пусть $x_1, \ldots, x_n$ — переменные ($n > 1$), K — нек-рая область целостности

Опр Выражение вида

$$f(x_1, \ldots, x_n) = \sum_{\substack{(k_1, \ldots, k_n) \\ \cap \\ A}} a_{k_1, \ldots, k_n} x_1^{k_1} \ldots x_n^{k_n}$$

где $a_{k_1, \ldots, k_n} \in K$ (т н коэффициенты),

A — конечное мн-во упорядоченных наборов $(k_1, \ldots, k_n)$ целых неотрицательных чисел

называется многочленом от $x_1, \ldots, x_n$ с коэффициентами из K

Выражение под знаком суммы наз одночленом

Обозначение

Мн-во всех многочленов $f(x_1, \ldots, x_n)$ будем обозначать $K[x_1, \ldots, x_n]$.

Операции сложения и умножения многочленов из $K[x_1, \ldots, x_n]$ вводятся естественным образом

Так, например, чтобы перемножить два многочлена $f(x)$ и $g(x)$ нужно раскрыть скобки и привести подобные, при этом

$$(a\, x_1^{k_1} \cdot \ldots \cdot x_n^{k_n})(b\, x_1^{l_1} \cdot \ldots \cdot x_n^{l_n}) = ab\, x_1^{k_1+l_1} \cdot \ldots \cdot x_n^{k_n+l_n}$$

подобными считаются одночлены $a x_1^{k_1} \ldots x_n^{k_n}$ и $b x_1^{l_1} \cdot \ldots \cdot x_n^{l_n}$, если

$$(k_1, \ldots, k_n) = (l_1, \ldots, l_n)$$

т е

$$k_1 = l_1, \ldots, k_n = l_n$$

Опр Степенью одночлена $a x_1^{k_1} \ldots x_n^{k_n}$ называется целое неотрицательное число $k_1 + \ldots + k_n$

Степень многочлена определяется стандартным образом, т е равна максимуму степеней входящих в него одночленов

Обозначение $\deg f(x_1, .., x_n)$

Заметим, что ~~...~~

$$\deg(a(x_1, .., x_n)\, b(x_1, .., x_n)) =$$
$$= \deg(a(x_1, .., x_n)) + \deg(b(x_1, .., x_n))$$

где $a(x_1, .., x_n)$, $b(x_1, .., x_n)$ — одночлены

Теорема 1

Множество $K[x_1, .., x_n]$ является областью целостности и называется кольцом мн-в от переменных $x_1, .., x_n$ над K

~~Доказа~~
Доказательство теоремы 1

Неочевидным является лишь целостность этого кольца, т.е. отсутствие в нем делителей нуля. Для док-ва последнего необходимо понятие лексикографического порядка, указанное ниже

Опр Говорят, что одночлен $a x_1^{k_1} \ldots x_n^{k_n}$ старше $b x_1^{l_1} \ldots x_n^{l_n}$, если $k_1 > l_1$, или, если $k_1 = l_1$, $k_2 > l_2$ и т д

Обозначение

$$a x_1^{k_1} \ldots x_n^{k_n} \succ b x_1^{l_1} \ldots x_n^{l_n}$$

Заметим, что всякий многочлен $f(x_1, .., x_n)$ можно записать по старшинству входящих в его состав одночленов единственным образом

Лемма

Старший член произведения 2 многочленов равен произведению старших членов этих многочленов

Доказательство

Пусть $f = u_1 + .. + u_s$, $g = v_1 + v_2 + .. + v_t$, где v_i, u_i — одночлены, причем $u_1 \succ u_2 \succ .. \succ u_s$, $v_1 \succ v_2 \succ .. \succ v_t$

Тогда $f g = \sum_{i,j} u_i v_j = u_1 v_1 + .. + u_i v_j + ..$, при этом

$$u_1 v_1 \succ u_i v_j$$

т. к. либо $i>1$, либо $j>1$

Доказательство теоремы 1 (продолжение)

Пусть $f \neq 0$, $g \neq 0$. Тогда $u \neq 0$, $v \neq 0$ — их старшие одночлены

По лемме $uv \neq 0$ — старший член произведения $f \cdot g$

Значит, $f g \neq 0$, т. е. Теорема 1 доказана

Опр. Многочлен $f(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ называется однородным, если все составляющие его одночлены имеют одинаковую степень

Значение этой степени наз. степенью однородности этого многочлена

Пример $K = \mathbb{Z}$, $n = 3$

$f(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2$

$g(x_1, x_2, x_3) = x_1 x_2 x_3^2 + x_1^2 x_2 x_3$

} однородные мн-ны степени 2 и 3 соот.

Очевидно, что всякий многочлен можно представить и притом единственным образом, в виде суммы его однородных компонент

Пример $K = \mathbb{Z}$, $n = 3$

$f(x_1, x_2, x_3) = x_1^5 x_2 - x_1 x_3^2 - x_1^2 x_2^2 + x_1 x_2 x_3 + 2x_2^4 x_3^2 + x_1^2 x_2^2 x_3^2$

Имеем $\deg f(x_1, x_2, x_3) = 6$, поэтому

$f_1(x_1, x_2, x_3) = x_1^5 x_2 + 2x_2^4 x_3^2 + x_1^2 x_2^2 x_3^2$

$f_2(x_1, x_2, x_3) = -x_1^2 x_2^2$

$f_3(x_1, x_2, x_3) = -x_1 x_3^2 + x_1 x_2 x_3$

Нетрудно видеть, что произведение двух однородных многочленов степени k и l есть однородный многочлен степени $k+l$ (при док-ве используется отсутствие делителей нуля в $K[x_1, \dots, x_n]$)

Отсюда следует, что ~~степень произведения~~

$\deg f g = \deg f + \deg g$

(достаточно, разбив f и g в суммы однородных компонент, перемножить старшие однородные компоненты и воспользоваться предыдущим свойством

Замечание

Многочлен $f(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ можно представлять себе как многочлен относительно переменной x_n с коэффициентами из $K[x_1, \dots, x_{n-1}]$

Пример

$$f(x_1, \dots, x_n) = x_1^5 x_2 - x_1 x_2^2 - x_1^2 x_2^2 + x_1 x_2 x_3 + 2x_2^4 x_3^2 + x_1^2 x_2^2 x_3^2 =$$
$$= (2x_2^4 + x_1^2 x_2^2) x_3^2 + (x_1 x_2) x_3 + (x_1^5 x_2 - x_1 x_2^2 - x_1^2 x_2^2) =$$
$$= F(x_3) \in (K[x_1, x_2])[x_3]$$

Это позволяет строить кольцо многочленов от $x_1, \dots, x_n$ индуктивно

Свойства кольца многочленов от $x_1, \dots, x_n$ с коэффициентами из нек-рого поля F во многом напоминают св-ва кольца $F[x]$ (есть понятие НОД, НОК, неприводимости, а также верна теорема о факторизации (точнее, ее аналог))

Но есть и принципиальные отличия. Так, например, НОД и НОК нельзя находить по алгоритму Евклида. Еще одним примером является то, что многочлены над $\mathbb{C}$ степени более 1 могут быть неприводимыми, несмотря на то, что $\mathbb{C}$ – алгебраически замкнутое поле

Пример

$$x_1^2 + \dots + x_n^2 + (-1) \text{ неприводим над } \mathbb{C} \text{ при } n \geq 2$$

1.21 21. Диагонализируемые линейные операторы. Теорема о диагонализируемости линейного оператора с простым спектром. Критерий диагонализируемости.

§ 11. Евклидовы пространства

п. 1 Скалярное произведение

Пусть $F = \mathbb{R}$, т.е. V – векторное пр-во над $\mathbb{R}$

Опр Будем говорить, что в пр-ве V задано скалярное умножение векторов, если определено отображение из V^2 в $\mathbb{R}$, т.е. каждой упорядоченной паре векторов $x, y \in V$ поставлено в соответствие действительное число, обозначаемое (x, y) и называемое скалярным произведением векторов x, y; при этом:

1. $(x, y) = (y, x)$ для любых $x, y \in V$ — условие симметрии
2. $(k_1 x_1 + k_2 x_2, y) = k_1 (x_1, y) + k_2 (x_2, y)$ $\forall k_1, k_2 \in \mathbb{R};\ x_1, x_2, y \in V$ — условие линейности
3. $(x, x) > 0$ $\forall x \in V,\ x \neq 0$ — условие положит-ти

Замечание

Имеем $(0, y) = 0$ $\forall y \in V$ как следствие условия линейности.

Примеры

1. $V = \mathbb{R}^n$

Пусть $x = (x_1, \dots, x_n),\ y = (y_1, \dots, y_n) \in \mathbb{R}^n$

Положим $(x, y) = x_1 y_1 + \dots + x_n y_n$

Эта формула задает скалярное умножение, называемое стандартным.

2. $V = \mathbb{R}^2,\ x = (x_1, x_2),\ y = (y_1, y_2)$.

Положим
$$(x, y) = (x_1\ \ x_2) \cdot \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = (x_1 + 2x_2\ \ \ 2x_1 + 5x_2) \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = x_1 y_1 + 2x_2 y_1 + 2x_1 y_2 + 5x_2 y_2$$

Эта формула также задает скалярное умножение в $\mathbb{R}^2$.

1. Условие линейности выполнено
2. Условие симметричности также выполнено
3. $(x, x) = x_1^2 + 4x_1 x_2 + 5x_2^2 > 0$ $\forall x = (x_1, x_2) \neq [$
   т.к. $D = 4^2 - 4 \cdot 5 = -4 < 0$

<u>Опр.</u> Векторы $x, y \in V$ называются ортогональными, если $(x, y) = 0$

<u>Опр.</u> Система векторов $a_1, \dots, a_m$ пр-ва V наз. ортогональной, если

$$(a_i, a_j) = 0 \text{ при } i \neq j,\ i, j = (1, \dots, m).$$

<u>Теорема 1</u>

Ортогональная система векторов, не содержащая нулевых векторов, является линейно независимой

<u>Доказательство:</u>

Пусть векторы $a_1, \dots, a_m$ отличны от нулевого и образуют ~~ортогона~~льную систему.

Докажем их линейную независимость

Пусть $k_1 a_1 + \dots + k_m a_m = 0$. Докажем, что, например, $k_1 = 0$.

Умножим скалярно обе части рав-ва на a_1

$$0 = (k_1 a_1 + k_2 a_2 + \dots + k_m a_m, a_1) =$$
$$= k_1 (a_1, a_1) + k_2 \overbrace{(a_2, a_1)}^{\text{ортогон.}}{}^{=0} + \dots + k_m \overbrace{(a_m, a_1)}^{\text{ор-огон.}}{}^{=0} =$$
$$= k_1 (a_1, a_1)$$

По св-ву положит-ти т.к. $a_1 \neq 0$, $(a_1, a_1) > 0$, след-но $k_1 = 0$.

<u>п. 2</u> Евклидово пространство

<u>Опр.</u> Конечномерное векторное пр-во V над полем $\mathbb{R}$, в к-ром задана нек-рое скалярное умножение векторов, называется Евклидовым пространством

<u>Теорема 2</u>

Любое конечномерное векторное пр-во V над полем F можно превратить в евклидово пространство.

<u>Доказательство</u>

Пусть $\dim V = n$, $b_1, \dots, b_n$ – нек-рый базис V

Формула $(x, y) = x_1 y_1 + \dots + x_n y_n$ (где $\begin{pmatrix} x_1 \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ y_n \end{pmatrix}$ – столбцы координат векторов x, y в данном

Основная теорема о симметрических многочленах

Н. Н. Осипов
Сибирский федеральный университет (Красноярск)
e-mail: nnosipov@rambler.ru

§ 1. Основная теорема о симметрических многочленах

Пусть R — *область целостности*, т. е. коммутативное кольцо с единицей и без делителей нуля. Многочлен $f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ называется *симметрическим*, если он не изменяется при всевозможных перестановках переменных $x_1, \ldots, x_n$. Многочлены

$$s_k = s_k(x_1, \ldots, x_n) = \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} \prod_{j=1}^{k} x_{i_j}, \quad k = 1, \ldots, n,$$

называют *элементарными симметрическими многочленами* от переменных $x_1, \ldots, x_n$. Главное утверждение о симметрических многочленах выражает следующая

Теорема. *Всякий симметрический многочлен*

$$f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$$

представляется в виде

$$f(x_1, \ldots, x_n) = F(s_1(x_1, \ldots, x_n), \ldots, s_n(x_1, \ldots, x_n)),$$

где $F(y_1, \ldots, y_n) \in R[y_1, \ldots, y_n]$. Это представление единственно.

Нам понадобится

Лемма. *Если лексикографически старшие члены многочленов*

$$u(x_1, \ldots, x_n) = \prod_{k=1}^{n} s_k^{l_k}(x_1, \ldots, x_n), \quad v(x_1, \ldots, x_n) = \prod_{k=1}^{n} s_k^{m_k}(x_1, \ldots, x_n)$$

имеют одинаковые наборы показателей, то

$$(l_1, \ldots, l_n) = (m_1, \ldots, m_n).$$

Для любого невозрастающего набора показателей $(k_1, \ldots, k_n)$ найдётся многочлен $u(x_1, \ldots, x_n)$ указанного вида, лексикографически старший член которого имеет этот набор показателей.

Доказательство. Второе утверждение леммы вытекает из существования решения системы уравнений

$$l_i + \ldots + l_n = k_i, \quad i = 1, \ldots, n,$$

в целых неотрицательных числах. Первое утверждение является следствием единственности такого решения: $l_i = k_i - k_{i+1}$, $i = 1, \ldots, n-1$, и $l_n = k_n$. $\square$

Доказательство теоремы. I. Существование. Присвоим каждому одночлену

$$a\prod_{i=1}^{n} x_i^{k_i} \tag{$*$}$$

натуральный номер по следующему правилу: одночлены нулевой степени получают номер 1, затем нумеруются одночлены первой степени в порядке лексикографического возрастания последних (при этом пропорциональные одночлены получают одинаковые номера), далее аналогично поступаем с одночленами второй степени и т. д. Будем дополнительно предполагать данный симметрический многочлен $f(x_1, \ldots, x_n)$ *однородным*; утверждение теоремы докажем индукцией по номеру m лексикографически старшего члена многочлена $f(x_1, \ldots, x_n)$.

При $m = 1$ доказывать нечего. Пусть утверждение доказано для всех номеров, меньших некоторого $m > 1$, и $f(x_1, \ldots, x_n)$ — произвольный однородный симметрический многочлен, лексикографически старший член $(*)$ которого имеет номер m. Рассмотрим многочлен

$$g(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) - a\prod_{k=1}^{n} s_k^{l_k}(x_1, \ldots, x_n)$$

где набор показателей $(l_1, \ldots, l_n)$ подобран так, что лексикографически старший член произведения

$$a\prod_{k=1}^{n} s_k^{l_k}(x_1, \ldots, x_n)$$

совпадает с $(*)$ (см. второе утверждение леммы). Нетрудно видеть, что многочлен $g(x_1, \ldots, x_n)$ — либо нулевой, либо однородный и симметрический, причем его лексикографически старший член имеет номер, меньший m. Осталось воспользоваться предположением индукции.

II. Единственность. Пусть есть ещё одно представление

$$f(x_1, \ldots, x_n) = G(s_1(x_1, \ldots, x_n), \ldots, s_n(x_1, \ldots, x_n)),$$

где $G(y_1, \ldots, y_n) \in R[y_1, \ldots, y_n]$. Предположим, что многочлен

$$H(y_1, \ldots, y_n) = F(y_1, \ldots, y_n) - G(y_1, \ldots, y_n)$$

оказался ненулевым, и пусть

$$U_t(y_1, \ldots, y_n), \quad t = 1, \ldots, N,$$

— все составляющие его одночлены. По первому утверждению леммы лексикографически старшие члены многочленов

$$u_t(x_1, \ldots, x_n) = U_t(s_1(x_1, \ldots, x_n), \ldots, s_n(x_1, \ldots, x_n))$$

попарно не пропорциональны. Но тогда самому старшему из них после приведения подобных в сумме

$$\sum_{t=1}^{N} u_t(x_1, \ldots, x_n) = H(s_1(x_1, \ldots, x_n), \ldots, s_n(x_1, \ldots, x_n))$$

не с чем будет сократиться — противоречие. □

Приведённое здесь доказательство является, по-видимому, стандартным для учебной литературы (см., например, книги [1], стр. 87 — 91, и [2], стр. 221 — 223). Другое доказательство дано в книге [3], стр. 259 — 261. Третье доказательство (единственности представления) есть в книге [4], стр. 422, однако оно требует погружения области целостности R в алгебраически замкнутое поле.

На практике при выражении симметрических многочленов через элементарные симметрические многочлены обычно используется *метод неопределённых коэффициентов* (см. ниже пример 3). В некоторых частных случаях возможны и другие подходы.

Пример 1. *Степенные суммы*

$$p_k = p_k(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^k, \quad k = 1, 2, \ldots,$$

можно выразить через элементарные симметрические многочлены, используя следующую *рекуррентную формулу Ньютона*:

$$p_l - p_{l-1}s_1 + p_{l-2}s_2 - \ldots + (-1)^{l-1}p_1 s_{l-1} + (-1)^l l s_l = 0. \qquad (**)$$

Здесь $l = 1, 2, \ldots$ и $s_k = 0$ при $k > n$.

Будем называть формулу $(**)$ (l,n)-*формулой*. Очевидно, $(1,n)$-формула верна.

I. Докажем, что (n,n)-формула верна. Для этого рассмотрим многочлен

$$\begin{gathered} f(X) = \prod_{i=1}^{n}(X - x_i) = \\ = X^n - s_1X^{n-1} + \ldots + (-1)^{n-1}s_{n-1}X + (-1)^n s_n \in R[x_1, \ldots, x_n][X]. \end{gathered}$$

Ясно, что

$$f(x_i) = 0, \quad i = 1, \ldots, n.$$

Сложив эти n равенств, получим (n,n)-формулу.

II. Докажем, что (l,n)-формула верна при $l > n$. Для этого достаточно положить в (l,l)-формуле $x_{n+1} = \ldots = x_l = 0$, и она превратится в (l,n)-формулу.

III. Пусть $l < n$. Докажем, что из $(l,n-1)$-формулы и $(l-1,n-1)$-формулы следует (l,n)-формула. Обозначим через s_k^* и p_k^* элементарные симметрические многочлены и степенные суммы от переменных $x_1, \ldots, x_{n-1}$. (l,n)-формулу можно записать так:

$$\begin{multline} (p_l^* + x_n^l) - (p_{l-1}^* + x_n^{l-1})(s_1^* + x_n) + (p_{l-2}^* + x_n^{l-2})(s_2^* + x_n s_1^*) - \ldots + \\ + (-1)^{l-1}(p_1^* + x_n)(s_{l-1}^* + x_n s_{l-2}^*) + (-1)^l((l-1)+1)(s_l^* + x_n s_{l-1}^*) = 0. \end{multline}$$

Частично раскрывая скобки в левой части, получим

$$\begin{multline} \Big[p_l^* - p_{l-1}^*(s_1^* + x_n) + p_{l-2}^*(s_2^* + x_n s_1^*) - \ldots + \\ + (-1)^{l-1}p_1^*(s_{l-1}^* + x_n s_{l-2}^*) + (-1)^l(l-1)(s_l^* + x_n s_{l-1}^*)\Big] + \\ + \Big[x_n^l - x_n^{l-1}(s_1^* + x_n) + x_n^{l-2}(s_2^* + x_n s_1^*) - \ldots + \\ + (-1)^{l-1}x_n(s_{l-1}^* + x_n s_{l-2}^*) + \boxed{(-1)^l(s_l^*} + x_n s_{l-1}^*)\Big] = 0 \end{multline}$$

Выражение во вторых квадратных скобках — «телескопическое», оно равно $(-1)^l s_l^*$. Добавляя это к выражению в первых квадратных скобках, мы получим ровно то, что будет, если от левой части $(l,n-1)$-формулы отнять левую часть $(l-1,n-1)$-формулы, предварительно умноженную на x_n.

IV. Теперь для доказательства (l,n)-формулы при $l < n$ можно применить метод индукции (база индукции — $(1,n)$-формулы и (n,n)-формулы).

Другое доказательство формулы Ньютона см., например, в книге [2], стр. 225 — 226. Оно же переизлагается в статье [5], где есть и ссылки на другие доказательства.

Так, например, имеем

$$p_1 = s_1, \quad p_2 = s_1^2 - 2s_2, \quad p_3 = s_1^3 - 3s_1s_2 + 3s_3$$

и т. д.

Если R — кольцо целых чисел, то из формулы Ньютона вытекает возможность выразить элементарные симметрические многочлены через первые n степенных сумм, однако коэффициенты соответствующих выражений уже будут дробными. Например:

$$s_1 = p_1, \quad s_2 = \frac{p_1^2 - p_2}{2}, \quad s_3 = \frac{p_1^3 - 3p_1p_2 + 2p_3}{6}$$

и т. д. Как следствие, любой симметрический многочлен $f(x_1, \ldots, x_n)$ с рациональными коэффициентами можно представить в виде некоторого многочлена (также с рациональными коэффициентами) от степенных сумм $p_1, \ldots, p_n$. Нетрудно показать, что такое представление единственно. Это следует из теоремы и связано с тем, что степенные суммы $p_1, \ldots, p_n$ выражаются через элементарные симметрические многочлены «треугольно»:

$$p_k = (-1)^{k-1} k s_k + \Phi_k(s_1, \ldots, s_{k-1}), \quad k = 1, \ldots, n,$$

где Φ_k — многочлены с целыми коэффициентами.

Пример 2. Вычислим *кубические резольвенты Феррари и Эйлера* для уравнения 4-й степени

$$x^4 + ax^3 + bx^2 + cx + d = 0,$$

корни которого обозначим x_1, x_2, x_3, x_4.

I. Корнями резольвенты Феррари являются

$$z_1 = x_1x_2 + x_3x_4, \quad z_2 = x_1x_3 + x_2x_4, \quad z_3 = x_1x_4 + x_2x_3.$$

Нетрудно видеть, что

$$\begin{aligned} &z_1 + z_2 + z_3 = s_2 = b, \\ &z_1z_2 + z_1z_3 + z_2z_3 = s_1s_3 - 4s_4 = ac - 4d, \\ &z_1z_2z_3 = s_1^2 s_4 - 4s_2s_4 + s_3^2 = a^2d - 4bd + c^2. \end{aligned}$$

Следовательно, резольвента Феррари выглядит так:

$$z^3 - bz^2 + (ac - 4d)z - (a^2d - 4bd + c^2) = 0.$$

Метод Феррари состоит в том, чтобы записать данное уравнение в виде

$$(x^2 + ax/2 + z/2)^2 + \ldots = 0,$$

где $z = z_i$ — один из корней резольвенты Феррари. В частности, для уравнения

$$x^4 + (\alpha + \gamma)x^3 + (\alpha\gamma + \beta + \delta)x^2 + (\alpha\delta + \beta\gamma)x + \beta\delta = 0,$$

которое приводится к виду

$$(x^2 + \alpha x + \beta)(x^2 + \gamma x + \delta) = 0,$$

одним из корней кубической резольвенты будет $\beta + \delta$.

II. Корни резольвенты Эйлера — это

$$\begin{aligned} w_1 &= (x_1 + x_2 - x_3 - x_4)^2, \\ w_2 &= (x_1 - x_2 - x_3 + x_4)^2, \\ w_3 &= (x_1 - x_2 + x_3 - x_4)^2. \end{aligned}$$

Имеем

$$\begin{aligned}
&w_1 + w_2 + w_3 = 3s_1^2 - 8s_2 = 3a^2 - 8b,\\
&w_1w_2 + w_1w_3 + w_2w_3 = 3s_1^4 - 16s_1^2s_2 + 16s_1s_3 + 16s_2^2 - 64s_4 =\\
&= 3a^4 - 16a^2b + 16ac + 16b^2 - 64d,\\
&w_1w_2w_3 = (s_1^3 - 4s_1s_2 + 8s_3)^2 = (a^3 - 4ab + 8c)^2,
\end{aligned}$$

и резольвента Эйлера такова:

$$w^3 - (3a^2 - 8b)w^2 + (3a^4 - 16a^2b + 16ac + 16b^2 - 64d)w - (a^3 - 4ab + 8c)^2 = 0.$$

§2. Дискриминант и результант

Не будем изобретать велосипед, а просто возьмём учебник [2], где на стр. 226 — 231 есть всё, что нужно знать про *дискриминант* и *результант*.

Пример 3. Вычислим дискриминант $D(f)$ кубического многочлена

$$f(x) = x^3 + ax + b.$$

По определению имеем

$$D(f) = [(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)]^2,$$

где x_1, x_2, x_3 — корни $f(x)$. Следовательно,

$$D(f) = x_1^4x_2^2 + \ldots = s_1^2s_2^2 + As_1^3s_3 + Bs_2^3 + Cs_1s_2s_3 + Ds_3^2.$$

Составив и затем решив систему линейных уравнений, найдём

$$A = -4, \quad B = -4, \quad C = 18, \quad D = -27.$$

Таким образом,

$$D(f) = s_1^2s_2^2 - 4s_1^3s_3 - 4s_2^3 + 18s_1s_2s_3 - 27s_3^2 = -4a^3 - 27b^2,$$

поскольку $s_1 = x_1 + x_2 + x_3 = 0$.

Список литературы

[1] *Винберг Э.Б.* Алгебра многочленов. М.: Просвещение, 1980.

[2] *Кострикин А.И.* Введение в алгебру. Ч. I. Основы алгебры. М.: Физико-математическая литература, 2000.

[3] *Кострикин А.И.* Введение в алгебру. М.: Наука, 1977.

[4] *Ляпин Е.С., Евсеев А.Е.* Алгебра и теория чисел. Ч. II. М: Просвещение, 1978.

[5] *Райхштейн З.Б.* Тождества Ньютона и математическая индукция // Математическое просвещение. Третья серия. Вып. 4. М.: МЦНМО, 2000. С. 204 — 205.

1.22 TODO 22. Квадратичные формы. Приведение квадратичной формы к сумме квадратов с коэффициентами методом Лагранжа.