Содержание

1 Линейная алгебра.

1.0.1 Вступление. Система линейных уравнений. Векторы.

Пусть K — фиксированное поле. Под линейным уравнением с неизвестными $x_1, \ldots, x_n$ будем подразумевать уравнение вида

$$a_1x_1 + \ldots + a_nx_n = b, a_i, b \in K.$$

Линейное уравнение называется однородным, если $b = 0$.

Система линейных уравнений

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + \ldots + a_{2n}x_n = b_2 \\ \ldots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = b_m \end{cases} . \tag{1}$$

Рассмотрим матрицу системы $A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{12} & \ldots & a_{mn} \end{pmatrix}$.

Определение 1 *Система уравнений называется совместной, если она имеет хотя бы одно решение, и несовместной в противном случае.*

Системы уравнений называются эквивалентными, если множества их решений совпадают.

Заметим, что системы, полученные друг из друга при помощи следующих действий будут эквивалентными.

1. Умножение строки на число, отличное от нуля.
2. Прибавление к одной строке другой, умноженной на любое число.
3. Перемена строк местами.

Данные преобразования будем называть элементарными.

Матрица, столбец. Умножение матрицы на столбец. Линейная комбинация столбцов. К более строгому определению этих понятий мы подойдем чуть позже.

1.1 Векторные пространства. Подпространства. Линейные комбинации. базис. Размерность.

Пусть K — поле.

Определение 2 *Векторным(линейным) пространством над полем K называется множество V с операциями сложения $+ : V \times V \longrightarrow V$ и умножения на элементы поля K $\cdot : K \times V \longrightarrow V$, обладающими следующими свойствам:*

1. *V абелева группа относительно сложенияю;*
2. *$\lambda(v + u) = \lambda v + \lambda u$ для всех $\lambda \in K$, $u, v \in V$;*
3. *$(\lambda + \mu)v = \lambda v + \mu v$ для всех $\lambda, \mu \in K$, $v \in V$;*
4. *$(\lambda\mu)v = \lambda(\mu v)$ для всех $\lambda, \mu \in K$, $v \in V$;*
5. *$1v = v$ для любого $v \in V$.*

Элементы векторного пространства будем называть векторами, а элементы поля K числами или скалярами.

Примеры.

1. K^n — пространство столбцов длины n.
2. Пространство строк длины n. Элементы пространства строк часто будем называть ковекторами.
3. $\mathbb{C}$ над $\mathbb{R}$.
4. $\mathbb{R}$ над $\mathbb{Q}$.
5. Пусть K, L — поля, причем $K \subset L$. В этом случае L/K будем называть расширением полей. Заметим, что L можно рассматривать как векторное пространство над полем K.
6. $K[x]$.
7. Пространство строк из элементов поля K бесконечной длины.
8. Пространство непрерывных функций на отрезке $[0, 1]$.

Определение 3 *Подмножество $U \subseteq V$ векторного пространства V называется подпространством, если оно само является векторным пространством относительно тех же операций, которые заданы на V.*

Лемма 1 *Подмножество $U \subseteq V$ является подпространством в том и только в том случае, если $u + v, \alpha u \in U$ для любых $u, v \in U, \alpha \in K$.*

1.1.1 Линейная комбинация. Базис. Размерность.

Определение 4 *Пусть $u_1, \ldots, u_n \in V$. Линейной комбинацией векторов $u_1, \ldots, u_n$ называется сумма*

$$\sum_{k=1}^{n} \alpha_i u_i,$$

где $\alpha_1, \ldots, \alpha_n \in K$.

Определение 5

- *Линейная оболочка множества векторов X есть наименьшее подпространство, содержащее X. Оно обозначается $\langle X \rangle$ и $\langle X \rangle = \cap_{X \subseteq U, U \leqslant V} U$.*
- *Множество X называется системой образующих пространства V, если $\langle X \rangle = V$.*
- *Пространство называется конечномерным, если у него есть система образующих из конечного числа векторов.*

Лемма 2 $\langle S \rangle = \{\sum_{k=1}^{n} \alpha_k u_k | u_1, \ldots, u_n \in S, \alpha_1, \ldots, \alpha_n \in K\}$.

Лемма 3 *Если вектор v является линейной комбинацией векторов из множества S, то $\langle S \rangle = \langle S \cup \{v\} \rangle$.*

1.1.2 Базис. Размерность.

Определение 6

- *Векторы $u_1, \ldots, u_n$ называются линейно зависимыми, если существует нетривиальная линейная комбинация этих векторов, равная нулю. В противном случае векторы $u_1, \ldots, u_n$ называются линейно независимыми.*
- *Базисом называется линейно независимая система образующих.*

Remark 1 *Набор векторов линейно зависим тогда и только тогда, когда хотя бы один из низ является линейной комбинацией остальных.*

Часто, когда говорят о базисе подразумевают упорядоченный набор векторов. Базисом нульмерного пространства будем считать пустое множество векторов.

Теорема 1 *(Эквивалентные определения базиса). Следующие условия на векторы $u_1, \ldots, u_n$ векторного пространства V эквивалентны.*

1. *$u_1, \ldots, u_n$ — базис.*
2. *$u_1, \ldots, u_n$ — максимальная линейно независимая система.*

3. $u_1, \ldots, u_n$ — *минимальная система образующих.*

4. *Для любого* $v \in V$ *существует единственный набор* $\alpha_1, \ldots, \alpha_n$ *такой, что* $v = \sum_{k=1}^{n} \alpha_i u_i$.

Доказательство. $1 \Longrightarrow 2$

Утверждение о том, что $u_1, \ldots, u_n$ — максимальная линейно независимая система означает, что любая система $u_1, \ldots, u_n, u_{n+1}, \ldots, u_n$ линейно зависима. Раз u_{n+1} по базису $u_1, \ldots, u_n$. $u_{n+1} = \sum_1^n \alpha_i u_i$. Тогда

$$u_{n+1} - \sum_1^n \alpha_i u_i = 0.$$

$2 \Longrightarrow 3$

Пусть v произвольный вектор пространства V. Система $u_1, \ldots, u_n, v$ линейно зависима, а значит

$$\sum_1^n \alpha_i u_i + \alpha v = 0 \tag{2}$$

для некоторых $\alpha_i, \alpha \in K$, среди которых не все равны 0. Если $\alpha = 0$, то из (2) получаем

$$\sum_1^n \alpha_i u_i = 0.$$

Откуда, в силу линейной независимости системы $u_1, \ldots, u_n$ все α_i равны 0. Значит $\alpha \neq 0$ и,

$$v = -\sum_1^n \frac{\alpha_i}{\alpha} u_i.$$

Таким образом $u_1, \ldots, u_n$ является системой образующих. Покажем, что $u_1, \ldots, u_n$ минимальная система образующих. Пусть $I \subset \{1, \ldots, n\}, I \neq \{1, \ldots, n\}$. Покажем, что система $\{u_i\}_{i \in I}$ не является системой образующих. Рассмотрим u_j, где $j \notin I$. Если $\{u_i\}_{i \in I}$ является системой образующих, то существуют такие $\alpha_i \in K$, что $u_j = \sum_{i \in I} \alpha_i u_i$, откуда $u_j - \sum_{i \in I} \alpha_i u_i = 0$, что противоречит линейной независимости $u_1, \ldots, u_n$.

$3 \Longrightarrow 4$

Пусть $v \in V$. Так как $u_1, \ldots, u_n$ система образующих, то существует набор $\alpha_1, \ldots, \alpha_n$ такой, что $v = \sum_{k=1}^{n} \alpha_i u_i$. Остается показать единственность такого набора. Предположим, что найдется два различных набора $\alpha_1, \ldots, \alpha_n$ и $\beta_1, \ldots, \beta_n$, что $v = \sum_{k=1}^{n} \alpha_i u_i = \sum_{k=1}^{n} \beta_i u_i$.

Тогда

$$\sum_{i=1}^{n}(\alpha_i - \beta_i)u_i = 0.$$

Поскольку наборя $\{\alpha_i\}$ и $\{\beta_i\}$ различны, то хотя бы одно из значений $\alpha_i - \beta_i$ не равно нулю. Для простоты дальнейших рассуждений предположим, что $\alpha_n - \beta_n \neq 0$. Тогда

$$u_n = \sum_{i=1}^{n-1} \frac{\alpha_i - \beta_i}{\alpha_n - \beta_n} u_i.$$

Откуда по лемме 3 набор векторов $u_1, \ldots, u_{n-1}$ тоже является системой образующих, что противоречит минимальности системы $u_1, \ldots, u_n$.

$4 \Longrightarrow 1$

Очевидно, что набор векторов $u_1, \ldots, u_n$ является системой образующих. Вектор $0 \in V$ единственным образом представим в виде $0 = \sum_{i=1}^{n} 0 \cdot u_i$. Отсюда следует, что векторы $u_1, \ldots, u_n$ линейно независимы.

□

Теорема 2 *(о существовании базиса). Пусть $X \subseteq Y \subseteq V$, причем X — линейна независима, а Y — система образующих. Тогда существует базис Z, содержащий X и содержащийся в Y.*

Доказательство.(см. [1, теорема 2.2]) Пусть

$$A = \{B : B - \text{линейно независима и } X \subseteq B \subseteq Y\}.$$

Всякое линейно упорядоченное (по включению) подмножество множества A имеет верхнюю грань (объединение). По лемме Цорна A содержит максимальный элемент Z.

Покажем, что Z — система образующих. Пусть $y \in Y \setminus Z$. Так как Z максимально, то $Z \cup \{y\}$ линейно зависимо, поэтому y является линейной комбинацией элементов из Z. Таким образом $\langle Z \rangle \supseteq \langle Y \rangle = V$.

□

Лемма 4 *(Лемма о замене) Пусть B — базис пространства V, $u \in B$, а вектор $v \in V$ не лежит в $\langle B \setminus \{u\} \rangle$. Тогда множество $\{B \setminus \{u\} \cup \{v\}\}$ также является базисом пространства V.*

Доказательство.(см. [1, лемма 3.1]) $\{B \setminus \{u\} \cup \{v\}\}$ — система образующих.

Т.к. B базис, то

$$v = \sum \alpha_i b_i + \alpha u,\ \alpha \neq 0 \tag{3}$$
$$u = \frac{1}{\alpha} v - \sum \alpha_i b_i \in \langle B \setminus \{u\} \cup \{v\}.$$

А, значит, $V = \langle B \rangle \subseteq \langle B \setminus \{u\} \cup \{v\} \rangle$.

$\{B \setminus \{u\} \cup \{v\}\}$ — линейно независима.

Пусть $\beta v + \sum \beta_i b_i = 0$, $b_i \neq u$. Подставим (3), получим

$$\alpha\beta u + \beta \sum \alpha_i b_i + \sum \beta_i b_i = 0.$$

А значит все коэффициенты этой линейной комбинации равны нулю, поэтому $\beta = 0$(т.к. $\alpha \neq 0$). А, значит и $\beta_i = 0$.

□

Теорема 3 *Любые два базиса пространства V равномощны.*

Доказательство. Здесь будет рассмотрен только случай конечномерного пространства. Для бесконечномерного случая теорема сохраняет силу. Пусть B и C два базиса и $|B| > |C| = n$. Применяя нужное количество раз лемму о замене получим, что система $B \setminus \{b_1, \ldots, b_n\} \cup C$ тоже является базисом, но $B \setminus \{b_1, \ldots, b_n\} \cup C \supseteq C$, что противоречит тому, что C максимальная линейно независимая система. □

Определение 7 *Количество элементов в базисе называется размерностью пространства*

Упражнение 1 *Найдите размерности пространств из примеров 1.1.*

Как мы увидим позже, всякое конечномерное векторное пространство изоморфно пространству K^n. Поэтому следующий пример является одним из важнейших.

Пример. Рассмотрим пространство столбцов K^n. Нетрудно проверить, что набор столбиков

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

является базисом K^n. Этот базис пространства K^n будем называть стандартным. Для вектора $x = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} \in K^n$ числа $\alpha_1, \ldots, \alpha_n$ являются координатами вектора x в стандартном базисе.

1.1.3 Бесконечномерный случай

Множество $X \subseteq V$ называется линейно независимым, если любой конечный набор векторов множество X линейно независим. Другими словами множество векторов линейно независимо если никакая конечная нетривиальная линейная комбинация его векторов не обращается в нуль.

Напомним, что в бесконечномерном случае верна теорема 3, т.е. любые два базиса пространства имеют одинаковую мощьность. примеры

Определение 8 *Пусть U подпространство векторного пространства V. Факторпространством V/U называется пространство, которое совпадает с V/U как абелева группа и с умножением на число, определенным с помощью формулы*

$$\alpha \cdot (v + U) = \alpha v + U.$$

Нетрудно убедиться, что V/U является векторным пространством.

1.2 Линейные отображения.

Гомоморфизмы векторных пространств называются линейными операторами или линейными отображениями. Изоморфизмом векторных пространств, как обычно, называется биективный гомоморфизм.

Определение 9 *Пусть V и U — векторные пространства над полем K. Отображение*

$$\varphi : V \longrightarrow U$$

называется линейным, если

1. $\varphi(x + y) = \varphi(x) + \varphi(y)$ *для любых* $x, y \in V$;
2. $\varphi(\lambda x) = \lambda\varphi(x)$ *для любых* $\lambda \in K$, $x \in V$.

Пусть $\varphi : V \longrightarrow U$ линейное отображение. Отметим очевидные свойства:

1. $\varphi(0) = 0$, $\varphi(-x) = -\varphi(x)$, $\varphi(x - y) = \varphi(x) - \varphi(y)$.

Примеры:

1. Поворот.
2. Ортогональное проектирование.
3. Дифференцирование в $K[x]$.
4. Проектор.

Определение 10 *Пусть V — векторное пространство над полем K и, одновременно, кольцо с той же операцией сложения. Если выполнено $\alpha(ab) = (\alpha a)b = a(\alpha b)$, $\forall a, b \in V, \alpha \in K$, то V называется алгеброй над полем K.*

Множество линейных отображений $V \longrightarrow V$ с операцией поточечного сложения, композиции и умножения на число является алгеброй с единицей. Эта алгебра обычно обозначается $\mathrm{End}(V)$. Мультипликативная группа кольца $\mathrm{End}(V)$ состоит из автоморфизмов пространства V и обозначается $\mathrm{GL}(V)$ или $\mathrm{Aut}(V), (\mathrm{End}(V))^*$.

1.2.1 Ядро линейного оператора. Размерность ядра и образа.

Пусть U и V — векторные пространства над полем K, $\varphi : U \longrightarrow V$ — линейное отображение.

$$\mathrm{Ker}\,\varphi = \{v \in U : \varphi(v) = 0\}, \qquad \mathrm{Im}\,\varphi = \{\varphi(v) : v \in U\}.$$

Нетрудно проверить, что $\mathrm{Ker}\,\varphi$ — подпространство U, а $\mathrm{Im}\,\varphi$ — подпространство V.

Упражнение 2 *Найти ядро и образ отображений из примеров.*

В силу определения линейное отображение является также гомоморфизмом соответвующих абелевых групп. Из уже известных нам фактом про абелевы группы следует следующее утверждение.

Предложение 1 *1. Линейно отображение $\varphi : U \longrightarrow V$ инъективно тогда и только тогда, когда $\mathrm{Ker}\,\varphi = 0$.*

2. Для любого $b \in V$ множество решений уравнения

$$\varphi(x) = b$$

имеет вид $a + \mathrm{Ker}\,\varphi$, где $a \in \varphi^{-1}(b)$.

Заметим также, что ядра линейных операторов и только они являются подпространствами векторного пространства. Множества вида $a+U = a+\mathrm{Ker}\,\varphi$, где $a \in V$, а U — подпространство V иногда называют аффинными.

1.2.2 Теорема о гомоморфизме. Размерность факторпространства.

Тем же способом, что и для групп можно доказать следующую теорему.

Теорема 4 *(Теорема о гомоморфизме для векторных пространств.)Пусть U и V — конечномерные векторные пространства над полем K, а $\varphi : U \longrightarrow V$ — линейное отображение. Тогда*

$$\operatorname{Im}\varphi \cong U/\operatorname{Ker}\varphi.$$

Лемма 5 *Пусть V — подпространство конечномерного пространства U. Тогда* $\dim V/U = \dim V - \dim U$.

Доказательство.

Пусть $u_1, \ldots, u_m$ — базис пространства U. Дополним его до базиса пространства V (это можно сделать по теореме о существовании базиса). Обозначим получившийся базис $u_1, \ldots, u_m, u_{m+1}, \ldots, u_n$. Пусть $\pi : V \longrightarrow V/U$ естественный эпиморфизм, т.е. $\pi(v) = v + U$. Для краткости обозначим $\bar{v} = \pi(v)$. Покажем, что все смежные классы $\overline{u}_{m+1}, \ldots, \overline{u}_n$ различны и образуют базис V/U.

линейная независимость:

Пусть

$$\sum_{i=m+1}^{n} \alpha_i \bar{u_i} = 0,$$

причем не все α_i равны нулю. Такое равенство означает, что $\sum_{i=m+1}^{n} \alpha_i u_i \in U$, а значит $\sum_{i=m+1}^{n} \alpha_i u_i = \sum_{i=1}^{n} \alpha_i u_i$. Последнее противоречит линейной независимости векторов $u_1, \ldots, u_n$.

Утверждение о том, что смежные классы $\overline{u}_{m+1}, \ldots, \overline{u}_n$ различны и порождают V/U доказывается еще проще. □

Размерность ядра и образа. Следующая теорема является следствием леммы 5 и теоремы о гомоморфизме.

Теорема 5 *Пусть U и V — конечномерные векторные пространства над полем K, а $\varphi : U \longrightarrow V$ — линейное отображение. Тогда*

$$\dim U = \dim \operatorname{Ker}\varphi + \dim \operatorname{Im}\varphi.$$

Для линейного отображения φ размерность его образа называется рангом отображения, т.е. $\operatorname{rk}\varphi = \dim \operatorname{Im}\varphi$.

1.3 Прямая сумма векторных пространств.

Сумма векторных пространств. Для подмножеств $U, V \subseteqq W$ будет обозначать $U + V = \{u + v | u \in U, v \in V\}$. Заметим, что если U и V являются подпространствами W, то $U + V, U \cap V$, а также, и $\cap_{i \in I} U_i$ любого семейстав подпространств тоже подпространство.

Напомним, что для подпространств U, W пространства V их сумма $U + W = \{u + w \mid u \in U, w \in W\}$ снова является подпространством. Аналогично можно определить и $U_1 + \ldots + U_n = \{u_1 + \ldots + u_n \mid u_i \in U_i, i = 1..n\}$ для подпространств $U_1, \ldots, U_n$. Стоит однако упомянуть, что объединение двух подпространств вовсе не обязательно является подпространством (приведите пример).

Лемма 6 *Пусть $U, W, U_1 \ldots, U_n$ подпространства V. Тогда*

1. $\langle \cup_{i=1}^n U_i \rangle = U_1 + \ldots + U_n$.
2. $U + W = W + U$;
3. $U + W = U \iff W \leqslant U$.

Прямая сумма векторных пространств.

Определение 11
- *Пространство V называется (внутренней) прямой суммой подпространств $U_1, \ldots, U_n$ и обозначается $V = U_1 \oplus \ldots \oplus U_n$, если каждый вектор $v \in V$ единственным образом представляется в виде $v = u_1 + \ldots + u_n$, где $u_i \in U_i$, $1 \leqslant i \leqslant n$.*
- *Пусть $U_1, \ldots, U_n$ — произвольные векторные пространства. Их (внешней) прямой суммой называется их декартово произведение $U_1 \times \ldots \times U_n$ с покомпонентными операциями.*

Лемма 7 *1. Сумма подпространств $U_1 + \ldots + U_n$ является прямой тогда и только тогда, когда*

$$0 = u_1 + \ldots + u_n,\ u_i \in U_i,\ 1 \leqslant i \leqslant n \Longrightarrow u_i = 0,\ 1 \leqslant i \leqslant n.$$

2. Сумма подпространств $U_1 + \ldots + U_n$ является прямой тогда и только тогда, когда

$$U_i \cap (U_1 + \ldots + U_{i-1} + U_{i+1} + \ldots + U_n) = 0,\ 1 \leqslant i \leqslant n.$$

3. Сумма подпространств $U + W$ является прямой тогда и только тогда, когда $U \cap W = \{0\}$.

Доказательство.

1. Импликация в одну сторону тривиальна. Покажем, что если 0 единственным образом представим в виде суммы векторов из U_i, то сумма U_i прямая. Пусть вектор v двумя способами представляется в виде $v = u_1 + \ldots + u_n = u'_1 + \ldots + u'_n$. Тогда $(u_1 - u'_1) + \ldots + (u_n - u'_n) = 0$, а значит $u_i = u'_i, \forall 1 \leqslant i \leqslant n$.

2. 2 Обозначим $W_i := U_1 + \ldots + U_{i-1} + U_{i+1} + \ldots + U_n$. Всякий вектор из $U_i \cap W_i$ двумя хотя бы способами представляется в виде суммы векторов из U_i, поэтому, если $U_i \cap W_i \neq \{0\}$, то сумма подпространств $U_1 + \ldots + U_n$ не является прямой. Обратно, пусть $U_i \cap W_i = \{0\}$, $\forall 1 \leqslant i \leqslant n$ и, пусть, $0 = u_1 + \ldots + u_n$, $u_i \in U_i$, причем не все u_i равны 0. Пусть $u_{i_1} \neq 0$, тогда $u_{i_1} = -\sum_{i \neq i_1} u_i \in U_{i_1} \cap W_{i_1}$, что противоречит тому, что $U_i \cap W_i = \{0\}$, $\forall 1 \leqslant i \leqslant n$.

3. Следует из предыдущего пункта.

□

Предложение 2 *1. (a) Пусть $V_1, \ldots, V_n$ — произвольные пространства. Отображения*

$$\begin{aligned} \mu_i : V_i &\longrightarrow V_1 \oplus \ldots \oplus V_n \\ v_i &\mapsto (0, \ldots, v_i, \ldots, 0) \end{aligned}$$

являются мономорфизмами (инъективными гомоморфизмами) векторных пространств.

(b) Если $V = V_1 \oplus \ldots \oplus V_n$, то внешняя пряма сумма пространств $V_1, \ldots, V_n$ изоморфна внутренней, т.е. V.

2. Если $V = V_1 \oplus \ldots \oplus V_n$, то объединение базисов подпространств V_i является базисом пространства V.

3. Если все пространства V_i конечноменры, то $\dim(V_1 \oplus \ldots \oplus V_n) = \sum_{i=1}^{n} \dim V_i$

Доказательство.

1. (a) .

   (b) Каждый вектор внутренней прямой суммы подпространств однозначно представляется в виде $v_1 + \ldots + v_n$, $v_i \in V_i$. Рассмотрим отображение $f(v_1 + \ldots + v_n) = (v_1, \ldots, v_n) \in V_1 \oplus \ldots \oplus V_n$. Оно является изоморфизмом.

2. Линейная независимость следует из определения прямой суммы и п.1. леммы 7.

3. Следует из предыдущего пункта.

Теорема 6 *(формула Грассмана) Пусть U, W — конечномерные подпространства векторного пространства V. Тогда*

$$\dim(U+W) = \dim U + \dim W - \dim(U \cap W).$$

Доказательство.(см. [?, стр. 26])или ([1, стр 34]) Зададим линейное отображение φ из внешней прямой суммы $U \oplus W$ в V с помощью формулы $\varphi(u,w) = u + w$. Легко проверить, что $\operatorname{Im}\varphi = U + W$, $\operatorname{Ker}\varphi = \{(u,-u) | u \in U \cap W\} \cong U \cap V$. Теперь теорема следует из теоремы о размерности ядра и образа. □

1.4 Матрицы. Часть 1.

Определение 12 *Двумерный массив $m \times n$ элементов поля K называется матрицей размера m на n над K.*

Пусть $\mathrm{Mat}_{m\times n}(K)$ обозначает множество всех таких матриц. Вместо $\mathrm{Mat}_{n\times n}(K)$ будем писать $\mathrm{Mat}_n(K)$. В зависимости от контекста элемент матрицы A расположенный в i-й строке j-м столбце будет обозначаться a_{ij}, A_{ij} или a^i_j, A^i_j.

На множестве матриц $\mathrm{Mat}_{m\times n}(K)$ введем операции сложения и умножения на число. Для $\alpha \in K$ и $A, B \in \mathrm{Mat}_{m\times n}(K)$ положим

$$(A+B)_{ij} = a_{ij} + b_{ij};$$
$$(\alpha A)_{ij} = \alpha A_{ij}.$$

Нетрудно убедиться, что относительно введенных операций $\mathrm{Mat}_{m\times n}(K)$ является векторным пространством размерности mn над полем K.

Стандартным базисом этого пространства будем называть базис состоящий из матриц e^j_i, где e^j_i матрица из $\mathrm{Mat}_{m\times n}(K)$ у которой в i-й строке j-м столбце стоит 1, а на остальных местах 0. Легко проверить, что $A = \sum_{i,j=1}^{n,m} a^i_j e^j_i$ для любой $A \in \mathrm{Mat}_{m\times n}(K)$.

Отметим, что пространства строк и столбцов можно рассматривать как $\mathrm{Mat}_{1\times n}(K)$ и $\mathrm{Mat}_{n\times 1}(K)$ соответственно. Выше уже обсуждалось умножение матрицы размера m на n на столбец. Обобщим это определение

Произведением матрицы $A \in \mathrm{Mat}_{m\times n}(K)$ на матрицу $B \in \mathrm{Mat}_{n\times k}(K)$ называется матрица $C = AB \in \mathrm{Mat}_{m\times k}(K)$ определенная формулой

$$c_{ij} = \sum_{l=1}^{n} a_{il} b_{lj}.$$

В случае, когда количество столбцов левой матрицы не равно количеству строк правой, произведение матриц не определено. Заметим, что произведение матриц некоммутативно.

Теорема 7 *1. Произведение матриц обладает следующими свойствами: для любых матриц A, B, C и $\alpha \in K$, если определены соответствующие произведения, то*

$$(AB)C = A(BC);\ A(B+C) = AB + AC;\ (B+C)A = BA + CA;$$
$$\alpha(AB) = (\alpha A)B = A(\alpha B).$$

2. $\mathrm{Mat}_n(K)$ *с операциями сложения и умножения является кольцом с единицей.*

Доказательство

$$((AB)C)^i_j = \sum_k (\sum_l a^i_l b^l_k) c^k_j = \sum_k \sum_l a^i_l b^l_k c^k_j$$
$$(A(BC))^i_j = \sum_l a^i_l (\sum_k b^l_k c^k_j) = \sum_l \sum_k a^i_l b^l_k c^k_j.$$

Аналогично проверяются остальные утверждения теоремы. □

Единицу кольца $\mathrm{Mat}_n(K)$ будем обозначать символом E. Т.е.

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

Нулевой элемент кольца $\mathrm{Mat}_n(K)$ чаще всего будет обозначаться просто 0, но иногда будем писать $\mathbb{O}$. Кольцо матриц дает нам важный пример некоммутативного кольца (при $n > 1$).

Группа обратимых элементов кольца $\mathrm{Mat}_n(K)$ обозначается $\mathrm{GL}_n(K)$.

1.5 Линейные операторы. Связь с матрицами.

1.5.1 Классификация конечномерных векторных простарнств.

Лемма 8 *Пусть U — векторное пространство над полем K, а $e = (e_1, \dots, e_n)$ — базис U. Тогда имеется следующий изоморфизм век-*

торных пространств:

$$\varphi_e : U \longrightarrow K^n$$
$$u = \sum_{i=1}^{n} \alpha_i e_i \mapsto \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

Числа $\alpha_1, \ldots, \alpha_n$ называются координатами вектора $u = \sum_{i=1}^{n} \alpha_i e_i$ в базисе e.

Corollary 1 *Любое конечномерное векторное пространство V изоморфно $K^{\dim V}$. Все векторные пространства одной и той же размерности изоморфны.*

1.5.2 Связь линейных отображений и матриц.

Для удобства изложения введем следующие обозначения:

Пусть $e = (e_1, \ldots, e_n)$ — базис пространства V и $x \in V$. Тогда существует однозначно определенный набор чисел $\alpha_i \in K$ такой, что $x = \sum_{i=1}^{n} \alpha_i e_i$. Обозначим через x^e столбик $\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \in K^n$. Тогда последнее равенство удобно записать в виде

$$x = \begin{pmatrix} e_1 & \ldots & e_n \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = ex^e.$$

Линейные отображения.

Лемма 9 *Линейное отображение однозначно определяется образами базисных векторов. Другими словами, если $e = (e_1, \ldots, e_n)$ — базис пространсва U, а $f_1, \ldots, f_n$ — векторы пространства V, то существует единственное линейное отображение $\varphi : U \longrightarrow V$ такое, что $\varphi(e_i) = f_i$, $1 \leqslant i \leqslant n$.*

Доказательство. Пусть $\varphi : U \longrightarrow V$ линейное отображение. $e = (e_1, \ldots, e_n)$ — базис U. Тогда

$$\varphi(\sum_{i=1}^{n} \alpha_i e_i) = \sum_{i=1}^{n} \alpha_i \varphi(e_i).$$

С другой стороны, если $v_1, \ldots, v_n$ — произвольные векторы пространства V, то нетрудно убедиться, что отображение

$$\sum_{i=1}^{n} \alpha_i e_i \mapsto \sum_{i=1}^{n} \alpha_i v_i$$

является линейным и переводит e_i в v_i. $\square$

Лемма 10 *Пусть $e = (e_1, \ldots, e_n)$ — базис пространсва U, а $\varphi : U \longrightarrow V$ линейное отображение такое, что $\varphi(e_i) = f_i$, $1 \leqslant i \leqslant n$. Обозначим набор векторов $f = (f_1, \ldots, f_n)$.*

1. *φ инъективен тогда и только тогда, когда f линейно независим.*
2. *φ сюръективен тогда и только тогда, когда f — система образующих.*
3. *φ биективен тогда и только тогда, когда f — базис.*

Доказательство.

1.

$$f \text{ линейно зависим } \Longleftrightarrow$$

$$\Longleftrightarrow \exists \alpha_1, \ldots, \alpha_n : \text{ не все равные нулю } \sum_{i=1}^{n} \alpha_i \varphi(e_i) = 0 \Longleftrightarrow$$

$$\Longleftrightarrow \exists \alpha_1, \ldots, \alpha_n : \varphi(\sum_{i=1}^{n} \alpha_i e_i) = 0 \Longleftrightarrow 0 \neq \sum_{i=1}^{n} \alpha_i e_i \in \operatorname{Ker} \varphi \Longleftrightarrow$$

$$\Longleftrightarrow \varphi \text{ не инъективен.}$$

2.

$$\operatorname{Im} \varphi = \{f(u) | u \in U\} = \{f(\sum_{i=1}^{n} \alpha_i e_i) | \alpha_i \in K\} = \{\sum_{i=1}^{n} \alpha_i f(e_i) | \alpha_i \in K\} =$$

$$= \langle f(e_i) \rangle.$$

3. Следует из предыдущих пунктов.

Corollary 2 *Два конечномерных векторных пространства изоморфны тогда и только тогда, когда они имеют одинаковую размерность.*

Пусть в векторных пространствах U и V зафиксированы базисы $e = (e_1, \ldots, e_n)$ и $f = (f_1, \ldots, f_m)$. Поскольку всякий линейный оператор $a : U \longrightarrow V$ однозначно определяется образами базисных векторов, то оператор a однозначно определяется матрицей $a_e^f = \begin{pmatrix} a(e_1)^f & a(e_2)^f & \ldots & a(e_n)^f \end{pmatrix}$ и всякая матрица из $\operatorname{Mat}_{m \times n}(K)$ определяет соответствующий оператор.

Для строки векторов $u = (u_1, \ldots, u_m)$ пространства U и линейного оператора $\varphi : U \longrightarrow V$ положим $\varphi(u) = (\varphi(u_1), \ldots, \varphi(u_m))$.

Предложение 3 *Пусть $e = (e_1, \ldots, e_n)$ — базис U, $f = (f_1, \ldots, f_m)$ — базис V.*

1. *Пусть* $\varphi : U \longrightarrow V$ *— линейное отображение. Тогда существует и единственная матрица* $A \in \mathrm{Mat}_{m\times n}(K)$ *такая, что для любого* $u \in U$ *имеет место равенство*
$$(\varphi(u))^f = Au^e.$$

2. *Для всякой матрицы* $A \in \mathrm{Mat}_{m\times n}(K)$ *соотношение* $(\varphi(u))^f = Au^e$ *определяет линейное отображение* $\varphi : U \longrightarrow V$.

Доказательство.

1. Рассмотрим $A = \begin{pmatrix}\varphi(e_1)^f & \varphi(e_2)^f & \dots & \varphi(e_n)^f\end{pmatrix}$. В силу линейности φ нетрудно проверить, что
$$(\varphi(u))^f = (\varphi(eu_e))^f = (\varphi(e)u_e)^f = Au_e.$$
Единственность матрицы A очевидна.
2. Следует из леммы 8.

□

Матрица A из последнего предложения называется матрицей отображения φ в базисах e и f. Иногда мы будем обозначать ее φ_e^f или просто φ_e, в случае, если $e = f, U = V$.

Примеры.

1. Поворот на плоскости на угол φ задается матрицей $\begin{pmatrix}\cos\varphi & -\sin\varphi\\ \sin\varphi & \cos\varphi\end{pmatrix}$.
2. Пусть $V = U \oplus W$, рассмотрим отображение
$$\varphi : V \longrightarrow V$$
$$(u, w) \mapsto u.$$
Заметим, что φ — линейное отображение, причем $\varphi^2 = \varphi$, $\mathrm{Im}\,\varphi = U$.
3. Дифференцирование многочленов не более чем 3-й степени. Рассмотрим базис $1, x, x^2, x^3$. Относительного выбранного базиса матрица оператора дифференцирования имеет вид: $\begin{pmatrix}0 & 1 & 0 & 0\\ 0 & 0 & 2 & 0\\ 0 & 0 & 0 & 3\\ 0 & 0 & 0 & 0\end{pmatrix}$.

Матрица композиции операторов

Предложение 4 *Матрица композиции линейных операторов является произведением матриц этих операторов. Точнее, если U, V и W — конечномерные векторные пространства с базисами e, f и g, соответственно, а $\varphi : U \longrightarrow V$ и $\psi : V \longrightarrow W$ — линейные отображения, то $(\psi \circ \varphi)_e^g = \psi_f^g \cdot \varphi_e^f$. В частности, при $U = V = W$ и $e = f = g$ получаем $(\psi \circ \varphi)_e = \psi_e \circ \varphi_e$.*

Доказательство.

$$((\psi \circ \varphi)_e^g)_j = ((\psi \circ \varphi)(e_j))^g = (\psi(\varphi(e_j)))^g = [] = \psi_f^g \cdot (\varphi(e_j))^f = \psi_f^g \cdot (\varphi_e^f)_j.$$

□

Предложения 3 и 4 можно переформулировать в виде следующей теоремы:

Теорема 8 *Пусть U и V — векторные пространства над полем K размерностей n и m соответственно пусть $e = (e_1, \ldots, e_n)$ — базис U, $f = (f_1, \ldots, f_m)$ — базис V. Тогда*

1. *Имеется изоморфизм между векторным пространством операторов $U \longrightarrow V$ и пространством матриц $\mathrm{Mat}_{m \times n}(K)$.*
2. *Имеется изоморфизм алгебр*

$$\mathrm{End}(U) \cong \mathrm{Mat}_n(K),$$
$$\varphi \mapsto \varphi_e.$$

Замена базиса. Матрица перехода. Очевидно, что изоморфизм из леммы 8 зависит от выбора упорядоченного базиса. Изучим как связаны координаты фиксированного вектора в двух различных базисах.

Пусть $e = (e_1, \ldots, e_n)$ — базис пространства V и $x \in V$.

$$x = \begin{pmatrix} e_1 & \ldots & e_n \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = ex^e.$$

Пусть $f = (f_1, \ldots, f_n)$ — другой базис пространства V. Разложим каждый из векторов базиса f по базису e. Пусть

$$f_i = \sum_{j=1}^{n} c_{ji} e_j, \ 1 \leqslant i \leqslant n.$$

Используя привычное обращение с матрицами последние равенства можно записать в виде

$$f = eC = \begin{pmatrix} e_1 & \dots & e_n \end{pmatrix} \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \dots & \dots & \dots & \dots \\ c_{n1} & c_{n2} & \dots & c_{nn} \end{pmatrix}.$$

Определение 13 *Матрица C называется матрицей перехода от базиса e к базису f и иногда мы будем обозначать ее C_f^e.*

Отметим, что в стобцах матрицы перехода стоят координаты "новых" базисных векторов в "старом" базисе. Т.е. $C_f^e = \begin{pmatrix} f_1^e & f_2^e & \dots & f_n^e \end{pmatrix}$. Легко видеть, что $C_e^e = E$.

Матрицу перехода C_e^f можно рассматривать как матрицу автоморфизма пространства V, переводящего базис e в базис f (в базисе e) или же как матрицу тождественного автоморфизма относительно базисов e и f (т.е. $C_e^f = (id)_e^f$).

Из предложения 3 следует следующая лемма.

Лемма 11 $C_e^f = (C_f^e)^{-1}$.

Наблюдения. Заметим, что если упорядоченный набор векторов $\mathbf{f} = (f_1, \dots, f_m)$ линейно независим, то для любых $a, b \in K^m$ равенство $\mathbf{f}a = \mathbf{f}b$ эквивалентно равенству $a = b$. Действительно,

$$\mathbf{f}a = \mathbf{f}b \Longleftrightarrow \mathbf{f}(a-b) = 0 \Longleftrightarrow a - b = 0 \Longleftrightarrow a = b.$$

Применяя полученное наблюдение к столбцам матриц, легко видеть, что для любых $A, B \in \mathrm{Mat}_{m\times n}(K)$ равенство $\mathbf{f}A = \mathbf{f}B$ эквивалентно равенству $A = B$.

Преобразование координат при замене базиса Пусть $\mathbf{f} = (f_1 \dots, f_n)$ и $e = (e_1, \dots, e_n)$ — базисы пространства V и v — произвольный вектор из V. Тогда

$$fv^f = v = ev^e = fC_e^f v^e.$$

Откуда в силу наблюдений предыдущего параграфа имеем

$$v^f = C_e^f v^e.$$

Последняя формула дает связь координат вектора в базисе f с его координатами в бвзисе e.

1.5.3 Изменение матрицы оператора при замене базиса.

Предложение 5 *Пусть e и e' — базисы пространства U, f и f' — базисы пространства V, $\varphi : U \longrightarrow V$ — линейное отображение. Тогда*

$$\varphi_{e'}^{f'} = C_f^{f'} \varphi_e^f C_{e'}^e.$$

Доказательство. В силу предложения 4

$$\varphi_{e'}^{f'} = (\mathrm{id} \circ \varphi \circ \mathrm{id})_{e'}^{f'} = (\mathrm{id} \circ \varphi)_e^{f'} \mathrm{id}_{e'}^e = \mathrm{id}_f^{f'} \varphi_e^f \mathrm{id}_{e'}^e = C_f^{f'} \varphi_e^f C_{e'}^e.$$

Но можно проверить и непосредственно

$$(\varphi_{e'}^{f'})_j = (\varphi(e'_j))^{f'} = C_f^{f'}(\varphi(e'_j))^f = C_f^{f'} \varphi_e^f (e'_j)^e = C_f^{f'} \varphi_e^f (C_{e'}^e)_j.$$

□

1.6 Решение системы линейных уравнений.

1.6.1 Решение системы линейных уравнений. Общий вид

В этом параграфе опишем множество решений системы линейных уравнений. Рассмотрим систему уравнений

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + \ldots + a_{2n}x_n = b_2 \\ \ldots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = b_m \end{cases} . \tag{4}$$

Рассмотрим матрицу системы $A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{12} & \ldots & a_{mn} \end{pmatrix}$. Ей соответствует линейное отображение

$$\varphi : K^n \longrightarrow K^m$$
$$x \mapsto Ax.$$

Легко проверить, что в стандартных базисах матрица отображения φ совпадает с A. Пусть $b = \begin{pmatrix} b_1 \\ \ldots \\ b_m \end{pmatrix} \in K^m$. Тогда наша система уравнений переписывается в виде

$$Ax = b.$$

Иными словами требуется найти $\varphi^{-1}(b)$.

Матрицу $(A|b)$ называют расширенной матрицей системы.

Как было показано выше, множество решений системы имеет вид $a+\operatorname{Ker}\varphi$, где a какое-нибудь решение системы $Ax = b$ (его обычно называют частным решением). В свою очередь $\operatorname{Ker}\varphi$ можно рассматривать как множество решений системы $Ax = 0$. Соответсвующую систему линейных уравнений называют однородной.

Таким образом для того, чтобы найти все решения системы (4) достаточно найти какое-нибудь одно ее решение и описать пространство $\operatorname{Ker}\varphi$. Для описания подпространства $\operatorname{Ker}\varphi$ достаточно найти базис этого пространства.

Определение 14 *Набор базисных векторов пространства* $\operatorname{Ker}\varphi$ *называется фундаментальной системой решений однородной системы уравнений.*

Как было показано выше $\dim\operatorname{Ker}\varphi = n-\operatorname{rk}\varphi$. Целью ближайших параграфов будет определение ранга оператора и описание фундаментальной системы решений.

1.6.2 Решение линейной системы уравнений. Элементарные преобразования. Метод Гаусса.

Следует отметить, что найти фундаментальную решений системы линейных уравнений проще всего когда матрица системы диагональна, и довольно просто когда матрица системы имеет треугольный вид, т.е., например, все ее элементы ниже главной диагонали нулевые. Для всякой системы линейных уравнений найдем эквивалентную ей систему со ступенчатой матрицей.

В параграфе 1.0.1 были перечислены элементарные преобразования системы линейных уравнений. Поскольку матричная запись гораздо удобнее, перейдем сразу на язык матриц. Будем работать с расширенной матрицей системы.

Определение 15 *Элементарными преобразованиями строк матрицы называются преобразования следующих типов:*

1. *прибавление к одной строке другой, умноженной на число;*
2. *умножение одной строки на число, отличное от нуля.*
3. *перестановка двух строк;*

Напомним, что стандартным базисом пространства матриц состоит из матриц e_i^j, где e_i^j матрица из $\operatorname{Mat}_{m\times n}(K)$ у которой в i-й строке j-м столбце стоит 1, а на остальных местах 0.

Каждое из элементарных преобразований равносильно домножению матрицы слева на обратимую матрицу.

- Прибавление к i-й строке j-й, умноженной на число α соответствует умножению слева на матрицу $E + \alpha e_i^j$.
- Умножение i-й строки на α соответствует умножению слева на матрицу $E + (\alpha - 1)e_i^i$.
- Перестановка i-й и j-й строк соответствует умножению слева на матрицу $E + e_i^j - e_i^i + e_j^i - e_j^j$.

Матрицы, имеющие вид $E + \alpha e_i^j$, где $\alpha \in K, i \neq j$ иногда называют трансвекциями, а матрицы вида $E + (\alpha - 1)e_i^i$ псевдоотражениями. Трансвекции и псевдоотражения будем называть элементарными матрицами.

Упражнение 3 *Покажите, что третье элементарное преобразование (перестановка строк) может быть получено с помощью конечного числа преобразований первых двух видов. Другими словами, матрица $E + e_i^j - e_i^i + e_j^i - e_j^j$ является произведением конечного числа элементарных матриц.*

Определение 16 *Ступенчатой будем называть матрицу у которой все нулевые строки (если они есть), стоят в конце, а номера первых ненулевых элементов строк строго возрастают.*

Ступенчатые матрицы имеют вид

$$\begin{pmatrix} 0 & \cdots & 0 & a^1_{j_1} & \ldots\ldots\ldots\ldots\ldots\ldots \\ 0 & \ldots\ldots\ldots & 0 & a^2_{j_2} & \ldots\ldots\ldots\ldots \\ 0 & \ldots\ldots\ldots\ldots\ldots & 0 & a^3_{j_3} & \ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ 0 & \ldots\ldots\ldots\ldots\ldots\ldots & 0 & a^m_{j_m} \end{pmatrix}.$$

Теорема 9 *1. Всякую матрицу можно привести к ступенчатому виду с помощью элементарных преобразований.*

2. Пусть $A \in \mathrm{Mat}(m, n, K)$. Тогда существуют такие $l \geqslant 0$ и элементарные матрицы $B_1, \ldots, B_l \in \mathrm{Mat}(m, m, K)$, что $B_1 \ldots B_l A$ — ступенчатая матрица.

Доказательство. Нулевая матрица - ступенчатая. Если матрица ненулевая, то пусть j_1 — номер первого ненулевого столбца. С помощью перестановки строк добьемся того, чтобы $a^1_{j_1} \neq 0$. Далее из каждой строки с номером $i \geqslant 2$ вычтем первую, умноженную на $\frac{a^i_{j_1}}{a^1_{j_1}}$, тем самым получив нули в j_1-м столбце

во всех строках, кроме первой. Далее рассмотрим получившуюся матрицу без первой строки и проделаем те же действия. □

Приведение матрицы к ступенчатому виду, изложенным выше способом, называется методом Гаусса. Для системы линейных уравнений, матрица которой ступенчатая, нетрудно написать частное решение и построить фундаментальную систему решений, тем самым описав все решения исходной линейной системы.

Отметим, что если после приведения системы к ступенчатому виду число ненулевых строк расширенной матрицы системы больше чем число ненулевых строк матрицы системы, то система не имеет решений.

1.7 Ранг оператора. Ранг матрицы.

1.7.1 Транспонирование матриц.

Определение 17 *Пусть* $A \in \mathrm{Mat}(m,n,K)$. *Матрица* $A^T \in \mathrm{Mat}(n,m,K)$ *с элементами* $(A^T)^i_j := A^j_i$ *называется транспонированной к* A.

Лемма 12 *1.* $(A+B)^T = A^T + B^T;\ (A^T)^T = A$.

2. $(AB)^T = B^T \cdot A^T$.

3. Если $A \in \mathrm{GL}(n,K)$, *то* $A^T \in \mathrm{GL}(n,K)$ *и* $(A^T)^{-1} = (A^{-1})^T$.

1.7.2 Ранг

Определение 18

- *Ранг системы векторов — размерность ее линейной оболочки.*
- *Ранг линейного оператора — размерность его образа.*
- *Ранг матрицы по строкам — ранг системы ее строк.*
- *Ранг матрицы по столбцам — ранг системы ее столбцов.*

Позднее будет показано, что ранг по строкам совпадает с рангом по столбцам, и будет называться просто рангом матрицы. Пусть $\mathrm{rk}_v A$ обозначает ранг матрицы A по столбцам, а $\mathrm{rk}_g A$ — по строкам. Из определений ясно, что $\mathrm{rk}_v A = \mathrm{rk}_g A^T$.

Предложение 6 *Пусть* $a : U \longrightarrow V$ *— линейное отображение,* e, f *— базисы пространств* U *и* V *соответственно. Тогда* $\mathrm{rk}\, a = \mathrm{rk}_v a^f_e$.

Доказательство. По лемме 10 $\mathrm{Im}\, a = \langle a(e_1)^f, \ldots, a(e_n)^f \rangle$, откуда следует утверждение.□

На ряду с элементарными преобразованиями строк, можно, также, в некоторых целях рассматривать преобразования столбцов.

Лемма 13 *1. Пространство, порожденное строками матрицы не изменяется при элементарных преобразованиях строк. Пространство, порожденное столбцами матрицы не изменяется при элементарных преобразованиях столбцов.*

2. *Ранг матрицы по строкам (столбцам) не меняется при элементарном преобразовании строк (столбцов).*

3. *Умножение матрицы на обратимую слева (справа) не меняет ее ранга по столбцам (строкам).*

4. *Ранг матрицы по столбцам не меняется при элементарном преобразовании строк.*

Доказательство.

1. Пусть $A^1, \ldots, A^n$ — строки матрицы A и пусть $U_1 = \langle A^1, \ldots, A^n \rangle, U_2 = \langle A^1, \ldots, A_i + \alpha A_j, \ldots, A^n \rangle$. Достаточно показать, что $U_1 = U_2$. Заметим, что $A^i = (A^i + \alpha A^j) - \alpha A^j$. Откуда по лемме 3 $U_1 = U_2$.

2. Следует из предыдущего пункта.

3. Обратимая матрица соответствует обратимому оператору. Произведению матриц соответствует композиция операторов. Таким образом, умножение матрицы оператора слева на обратимую матрицу соответствует замене базиса в его множестве значений, а справа — в области определения. Так как столбцовый ранг матрицы не зависит от выбора базиса, то столбцовый ранг не меняется при умножении на обратимую матрицу.

   (Формально: Пусть $B \in \mathrm{GL}(m, K), A \in \mathrm{Mat}(m, n, K)$. Рассмотрим оператор $K^m \longrightarrow K^m$, матрица которого в стандартном базисе есть B^{-1}. Так как матрица B^{-1} обратима, то в силу леммы 10 столбцы матрицы B^{-1}(обозначим их $f = (B_1^{-1}, \ldots, B_m^{-1})$) образуют базис пространства K^m. Матрица B тогда является матрицей тождественного оператора относительно стандартного базиса e и базиса f,(т.е. т.к. $E = B^{-1}B$, получаем, что $B = \mathrm{id}_e^f$). Пусть $a : K^n \longrightarrow K^m$ — оператор , для которого $a_g^e = A$ где g — стандартный базис K^n (т.е. $a(x) = Ax$). Тогда

   $$BA = \mathrm{id}_e^f \cdot a_g^e = (\mathrm{id} \circ a)_g^f = a_g^f,$$

   (последнее равенство следует из теоремы 4)). Таким образом $\mathrm{rk}(BA) = \mathrm{rk}(a_g^f) = \mathrm{rk}\, a = \mathrm{rk}\, A$.

   Следующее утверждение следует из того, что строчной ранг матрицы равен столбцовому рангу транспонированной к ней, а транспонированная к обратимой — обратима.

4. Утверждение следует из предыдущего пункта.

□

Corollary 3 *Ранг матрицы равен числу ненулевых строк любой ступенчатой матрицы, к которой она приводится элементарными преобразованиями строк.*

Доказательство. Достаточно показать, что ненулевые строки ступенчатой матрицы линейно независимы, а значит образуют базис пространства строк матрицы. □

Теорема 10 *Пусть* $A \in \mathrm{Mat}(m, n, K)$, *тогда* $\mathrm{rk}_v(A) = \mathrm{rk}_g(A)$.

Доказательство.(или см. [2, гл2 §2 теорема 1]) В силу теоремы 9 и леммы 13 достаточно проверить утверждение только для ступенчатой матрицы A. Пусть $\mathrm{rk}_g(A) = r$ и $j_1, j_2, \ldots, j_r$ — номера первых ненулевых элементов в строках $1, \ldots, r$. Применив необходимое число раз элементарное преобразование второго типа, можно считать, что $A^i_{j_i} = 1$, $1 \leqslant i \leqslant r$ и $A^k_{j_i} = 0$ при $k < i$. Далее тем же образом как это было проделано при приведении матрицы к ступенчатому виду при помощи элементарных преобразований над строками, можно с помощью элементарных преобразований столбцов (т.е. не меняя ни строчного не столбцового ранга) привести матрицу к виду

$$e^1_1 + \ldots + e^r_r = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 0 & 0 \end{pmatrix}.$$

Совсем просто убедиться в том, что ранг по строкам и ранг по столбцам для последней матрицы совпадают и равны r. □

Теорема 11 *(Теорема Кронекера-Капелли) Система линейных уравнений совместна тогда и только тогда, когда ранг матрицы ее коэффициентов равен рангу расширенной матрицы.*

Доказательство. Пусть $(A|b)$ — расширенная матрица системы линейных уравнений. $\mathrm{rk}\, A \leqslant \mathrm{rk}(A|b)$, причем $\mathrm{rk}\, A < \mathrm{rk}(A|b)$ тогда и только тогда, когда у ступенчатой матрицы для расширенной матрицы системы последняя ненулевая строчка имеет вид $\begin{pmatrix} 0 & \ldots & 0 & 1 \end{pmatrix}$, что означает несовместность исходной системы.

(Совместность системы $Ax = b$ эквивалентна условию $b \in \mathrm{Im}\, A$, где A — оператор с матрицей A в стандартных базисах. Последнее равносильно тому, что $\mathrm{rk}\, A = \mathrm{rk}(A|b)$.) □

Предложение 7 *Пусть* $A \in \mathrm{Mat}(n, K)$. *Тогда* A *обратима тогда и только тогда, когда* $\mathrm{rk}\, A = n$.

Доказательство.Пусть $a : K^n \longrightarrow K^n$ линейный оператор, для которого $a(x) = Ax$, т.е. $A = a_e^e$ для стандартного базиса e. Тогда $\mathrm{rk}\, A = n \iff \mathrm{rk}\, a = n \iff \dim \mathrm{Im}\, a = n \iff \begin{cases} \mathrm{Im}\, a = K^n \\ \mathrm{Ker}\, a = \{0\} \end{cases} \iff a$ — обратим, что эквивалентно тому, что матрица A обратима. □

1.8 Определитель матрицы. Форма объема.

1.8.1 Предисловие. Объем параллелепипеда.

(см. [2, гл.3]) Сопоставим квадратной матрице $A = (A_1, \ldots, A_n)$ параллелепипед, ребра которого задаются столбцами матрицы A.

$$\prod = \{x_1 A_1 + \ldots + x_n A_n | x_i \in [0, 1]\}.$$

Ориентированный объем n-мерного параллелепипеда определяется по индукции: $V^{(n)}(A) = V^{(n-1)}(A_1, \ldots, A_{n-1}) \cdot h_{A^n}$. В качестве примера рассмотрим площадь параллелограмма. Известно, что она обладает следующими свойствами:

1. $v(\Pi(A_1, A_2)) = -v(\Pi(A_2, A_1))$;
2. $v(\Pi(A_1 + A_3, A_2)) = v(\Pi(A_1, A_2)) + v(\Pi(A_3, A_2))$, $v(\Pi(\lambda A_1, A_2)) = \lambda v(\Pi(A_1, A_2))$;
3. $v(\Pi(E)) = 1$.

(второе свойство следует из того, что высота параллелепипеда есть длина проекции на прямую, ортогональную соответствующей стороне, а проектирование является линейным отображением.)

1.8.2 Пространства полилинейных отображений

$\mathrm{Multi}(V_1, \ldots, V_k, Y)$, $\mathrm{Multi}_k(V, Y)$. Пространства полилинейных форм $\mathrm{Multi}(V_1, \ldots, V_k, K)$, $\mathrm{Multi}_k V$.

V — векторное пространство над полем K.

Определение 19 $f : V \times \ldots \times V \longrightarrow K$ *полилинейное отображение(*m*-форма), если оно линейно по каждому аргументу, т.е. для любых* $u, v \in V$ *и* $\alpha \in K$ *выполнены равенства*

$$f(\ldots, u + v, \ldots) = f(\ldots, u, \ldots) + f(\ldots, v, \ldots)$$
$$f(\ldots, \alpha v, \ldots) = \alpha f(\ldots, v, \ldots).$$

Пусть $\mathrm{Multi}_k V$ обозначает пространство k-форм $V \times \ldots \times V \longrightarrow K$.

Непосредственно из определения полилинейности следует следующая лемма.

Лемма 14 *Пусть $e = (e_1, \ldots, e_n)$ — базис V, $f : V \times \ldots \times V \longrightarrow K$ — полилинейное отображение. Тогда*

$$f(v_1, \ldots, v_m) = \sum_{i_1,\ldots,i_m=1}^{n} f(e_{i_1}, \ldots, e_{i_m})(v_1^e)^{i_1} \ldots (v_m^e)^{i_m} =$$

$$= \sum_{i_1,\ldots,i_m=1}^{n} f(e_{i_1}, \ldots, e_{i_m}) a_1^{i_1} \ldots a_m^{i_m},$$

где $A = (v_1^e \ldots v_m^e)$.

Утверждение леммы означает, что полилинейная форма однозначно определяется m-мерным массивом своих значений на базисных векторах.

Примеры. Важным примером полилинейных отображений, который мы будем рассматривать позднее, являются билинейные формы $B : V \times V \longrightarrow K$. Одним из примеров билинейных форм служит скалярное произведение векторов на плоскости. В общем виде билинейная форма $f : K^n \times K^n \longrightarrow K$ имеет вид $f((x^1, \ldots, x^n)^T, (y^1, \ldots, y^n)^T) = \sum_{i,j=1}^{n} a_{ij} x^i y^j$.

Пространство симметричных полилинейных форм.

$$\mathrm{SMulti}_k V =$$
$$= \{\omega \in \mathrm{Multi}_k V \mid \omega(v_1 \ldots, v_i \ldots, v_j, \ldots, v_k) = \omega(v_1 \ldots, v_j \ldots, v_i, \ldots, v_k)\}.$$

Нетрудно проверить, что $\mathrm{SMulti}_k V$ является подпространством $\mathrm{Multi}_k V$.

Remark 2 *Определим действие симметрической группы S_k на $\mathrm{Multi}_k V$ следующим образом:*

$$S_k \times \mathrm{Multi}_k V \longrightarrow \mathrm{Multi}_k V$$
$$(\sigma\omega)(v_1, \ldots, v_k) = \omega(v_{\sigma(1)}, \ldots, v_{\sigma(k)}).$$

Упражнение 4 *Проверьте, что это действительно действие группы на множестве.*

Remark 3 *Пространство симмметричных полилинейных форм можно было бы определить как множество таких форм $\omega \in \mathrm{Multi}_k V$, что для всякой подстановки $u \in S_k$ выполнено $\omega(v_1 \ldots, v_k) = \omega(v_{u(1)} \ldots, v_{u(k)})$.*

Пространство антисимметричных полилин. форм.

$$\mathrm{AMulti}_k V = \{\omega \in \mathrm{Multi}_k V \mid \forall\, v_1, \ldots, v_k \in V \\ \big(\exists\, i, j \in \{1, \ldots, k\}\ (i \neq j \ \wedge\ v_i = v_j) \ \Rightarrow\ \omega(v_1, \ldots, v_k) = 0\big)\}.$$

Лемма 15 *1. Для всякой антисимммметричной полилинейной формы* $\omega \in \mathrm{Multi}_k V$ *выполнено*

$$\omega(v_1 \ldots, v_i \ldots, v_j, \ldots, v_k) = -\omega(v_1 \ldots, v_j \ldots, v_i, \ldots, v_k). \tag{5}$$

2. Если $\mathrm{char}\, K \neq 2$*, то из условия (5) следует антисимметричность формы.*

3. Для $w \in \mathrm{Multi}_n(V)$ *условие (5) эквивалентно тому, что для всех* $\sigma \in S_n$ *выполнено* $\omega(v_{\sigma(1)}, \ldots, v_{\sigma(k)}) = \mathrm{sgn}(\sigma)\omega(v_1, \ldots, v_k)$.

Доказательство.

1.

$$0 = \omega(\ldots, v_i{+}v_j, \ldots, v_i{+}v_j, \ldots) = \omega(\ldots, v_i, \ldots, v_i, \ldots){+}\omega(\ldots, v_i, \ldots, v_j, \ldots){+} \\ + \omega(\ldots, v, \ldots, u, \ldots) + \omega(\ldots, v, \ldots, v, \ldots) = \\ = \omega(\ldots, v_i, \ldots, v_j, \ldots) + \omega(\ldots, v_j, \ldots, v_i, \ldots) \Longrightarrow \\ \omega(\ldots, v_i, \ldots, v_j, \ldots) = -\omega(\ldots, v_j, \ldots, v_i, \ldots).$$

2. Достаточно подставить в условие (5) $v_i = v_j$.

3. Следует из предыдущего пункта и того, что всякая перестановка является произведением транспозиций, а транспозиция является нечетной перестановкой.

□

Лемма 16 *Пусть* ω *— полилинейное антисимметричное отображение. Тогда*

$$\omega(\ldots, v_i, \ldots, v_j, \ldots) = \omega(\ldots, v_i + \alpha v_j, \ldots, v_j, \ldots), \quad \forall \alpha \in K.$$

1.8.3 Формы объема.

Определение 20 *Антисимметричная полилинейная* n*-форма на* n*-мерном векторном пространстве называется формой объема.*

Лемма 17 *Пусть* $\omega : \underbrace{V \times \ldots \times V}_{n \text{ раз}} \longrightarrow K$ *полилинейная антисимметричная форма,* $e = (e_1, \ldots, e_n)$ *— базис* V*. Тогда*

$$\omega(v_1, \ldots, v_n) = \omega(e_1, \ldots, e_n) \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)(v_1^e)^{\sigma(1)} \ldots (v_n^e)^{\sigma(n)} =$$

$$= \omega(e_1, \ldots, e_n) \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_1^{\sigma(1)} \ldots a_n^{\sigma(n)},$$

где $A = (v_1^e \ldots v_n^e)$.

Доказательство. Применив лемму 14 остается только, воспользовавшись антисимметричностью формы ω.□

Определение 21 • *Скаляр* $\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_1^{\sigma(1)} \ldots a_n^{\sigma(n)}$ *назовем определителем матрицы* $A \in \operatorname{Mat}_n(K)$.

Лемма 18 *(см. [1, лемма 2.2.]) Определитель матрицы является полилинейной антисимметричной формой ее столбцов, а* $\det E = 1$.

Доказательство. Полилинейность, как и равенство $\det E = 1$, легко следует из определения. Докажем антисимметричность. Пусть столбцы A_k и A_l матрицы $A = (a_j^i)_{1 \leqslant i,j \leqslant n}$ совпадают. Покажем, что $\det A = 0$. Индекс знакопеременной группы $\mathcal{A}_n$ в S_n равен 2. Пусть $\tau = (kl)$, тогда $S_n = \mathcal{A}_n \cup \mathcal{A}_n\tau$.

$$\det A = \sum_{\sigma \in S_n} (-1)^{\operatorname{sgn}(\sigma)} \prod_{i=1}^n a_i^{\sigma(i)} = \sum_{\sigma \in A_n} \prod_{i=1}^n a_i^{\sigma(i)} - \sum_{\rho \in A_n\tau} \prod_{i=1}^n a_i^{\rho(i)} =$$

$$= \sum_{\sigma \in \mathcal{A}_n} \prod_{i=1}^n a_i^{\sigma(i)} - \sum_{\sigma \in \mathcal{A}_n} \prod_{i=1}^n a_i^{\sigma\tau(i)} = \sum_{\sigma \in \mathcal{A}_n} \prod_{i=1}^n a_i^{\sigma(i)} - \sum_{\sigma \in \mathcal{A}_n} a_k^{\sigma\tau(k)} a_l^{\sigma\tau(l)} \prod_{i \neq k,l}^n a_i^{\sigma(i)} =$$

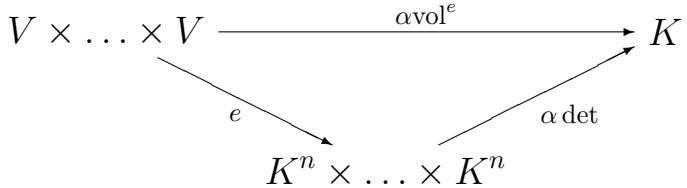
$$= \sum_{\sigma \in \mathcal{A}_n} \prod_{i=1}^n a_i^{\sigma(i)} - \sum_{\sigma \in \mathcal{A}_n} a_k^{\sigma(l)} a_l^{\sigma(k)} \prod_{i \neq k,l}^n a_i^{\sigma(i)} = 0.$$

Последнее равенство следует из того, что $a_l^i = a_k^i$, $1 \leqslant i \leqslant n$. □

Утверждение леммы означает, что определитель является формой объема на пространстве K^n.

Для каждого базиса определим форму объема, связанную с базисом: $\operatorname{vol}^e(v_1, \ldots, v_n) = \det\left(v_1^e \ \ldots \ v_n^e\right)$.

Данная диаграмма служит иллюстрацией излагаемого:



В следующей теореме перечислены простые или уже доказанные факты о формах объема.

Теорема 12 *(Теорема о формах объема.) Пусть K — поле, V — векторное пространство над полем K , $n = \dim V < \infty$ и e — базис V. Тогда*

1. *$vol^e(e_1, \dots, e_n) = 1$ и vol^e является формой объема на V;*
2. *для любой формы объема ω на V и базиса e выполнено $\omega = \omega(e_1, \dots, e_n)\, vol^e$. Таким образом любая форма объема пропорциональна определителю.*

   Для любого базиса $\tilde{e}$ пространства V выполнено $vol^{\tilde{e}} = \det \mathrm{c}_e^{\tilde{e}} \cdot vol^e$;
3. *Множество форм объема на данном векторном пространстве является одномерным векторным пространством.*
4. *(a) Пусть ω ненулевая форма объема на V. Тогда набор векторов $v_1, \dots, v_n \in V$ является базисом, если и только если $\omega(v_1, \dots, v_n) \neq 0$.*

   (b) Определитель квадратной матрицы не равен нулю тогда и только тогда, когда ее строки (столбцы) линейно независимы.

   (c) Матрица $A \in \mathrm{Mat}(n, K)$ обратима тогда и только тогда, когда ее определитель не равен нулю. Т.е. $\mathrm{GL}(V) = \{a \in \mathrm{End}(V) | \det a \neq 0\}$.

Доказательство. Первые два утверждения уже доказаны выше. Третье утверждение следует из второго.

Докажем утверждение (4 а):$\omega \neq 0$, а значит $\exists x_1, \dots, x_n \in V : \omega(x_1, \dots, x_n) \neq 0$.

$\Longrightarrow$

Если набор векторов $v_1, \dots, v_n \in V$ является базисом, то $\omega(x_1, \dots, x_n) = \omega(v_1, \dots, v_n)\mathrm{vol}^v(x_1, \dots, x_n)$. Следовательно, $\omega(v_1, \dots, v_n) \neq 0$.

$\Longleftarrow$

Если набор векторов $v_1, \dots, v_n \in V$ не является базимом, то один из элементов выражается в виде линейной комбинации остальных, скажем, $v_i = \sum_{j \neq i} \alpha_j v_j$. Тогда по лемме 16 получаем, что $\omega(v_1, \dots, v_n) = 0$.

Пункт (4б) уже был доказан (см. предложение 7), но подчеркнем, что он, в частности, следует из (4a), как и п. (4c). □

Remark 4 *Из всего сказанного выше следует, что есть только одна полилинейная антисимметрическая функция $f : \mathrm{Mat}(K, n) \longrightarrow K$ столбцов квадратной матрицы, для которой $f(E) = 1$, и это определитель.*

Предложение 8 *Пусть $a \in \mathrm{End}(V)$, ω — форма объема на V. Тогда*

1. *Функция $\omega_a : \underbrace{V \times \ldots \times V}_{n\ раз} \longrightarrow K$, заданная равенством $\omega_a(x_1, \ldots, x_n) = \omega(a(x_1), \ldots, a(x_n))$ является формой объема.*
2. *Значение выражения $\frac{\omega(a(e_1),\ldots,a(e_n))}{\omega(e_1,\ldots,e_n)}$, где ω — ненулевая форма объема, а $e_1, \ldots, e_n$ — базис пространства V, не зависит ни от формы ω ни от базиса.*
3. *Пусть A матрица оператора a в базисе $e_1, \ldots, e_n$. Тогда $\det A = \mathrm{vol}^e(a(e_1), \ldots, a(e_n)) = \frac{\omega(a(e_1),\ldots,a(e_n))}{\omega(e_1,\ldots,e_n)}$.*

Доказательство. Первое утверждение проверяется непосредственно. Перейдем ко второму. Отметим сперва, что в силу пункта 4 предыдущей теоремы $\omega(e_1, \ldots, e_n) \neq 0$.

Покажем сперва, что значение $\frac{\omega(a(e_1),\ldots,a(e_n))}{\omega(e_1,\ldots,e_n)}$ не зависит от формы ω. По теореме о формах объема, пространство форм объема одномерно, поэтому форма ω образует его базис. Это означает, что для всякой формы объема $\widetilde{\omega}$ существует $c \in K$ такой, что $\widetilde{\omega} = c\omega$. Таким образом

$$\frac{\widetilde{\omega}(a(e_1), \ldots, a(e_n))}{\widetilde{\omega}(e_1, \ldots, e_n)} = \frac{c\omega(a(e_1), \ldots, a(e_n))}{c\omega(e_1, \ldots, e_n)} = \frac{\omega(a(e_1), \ldots, a(e_n))}{\omega(e_1, \ldots, e_n)} \tag{6}$$

Осталось показать, что $\frac{\omega(a(e_1),\ldots,a(e_n))}{\omega(e_1,\ldots,e_n)}$ не зависит от выбора базиса. Пусть $\tilde{e}_1, \ldots, \tilde{e}_n$ — базис V. Снова, поскольку форма ω образует базис пространства форм объема, найдется такой $d \in K$, что $\omega_a = d\omega$, а значит

$$\frac{\omega(a(\widetilde{e}_1), \ldots, a(\widetilde{e}_n))}{\omega(\widetilde{e}_1, \ldots, \widetilde{e}_n)} = \frac{d\omega(\widetilde{e}_1, \ldots, \widetilde{e}_n)}{\omega(\widetilde{e}_1, \ldots, \widetilde{e}_n)} = d.$$

Докажем последний пункт. Первое равенство следует из определения формы vol^e, а для доказательства второго достаточно подставить $\omega = \mathrm{vol}^e$, т.к. независимость правой части от формы уже доказана.

□

Определение 22 *Определителем линейного оператора $a \in \mathrm{End}(V)$ назовем $\det a = \frac{\omega(a(e_1),\ldots,a(e_n))}{\omega(e_1,\ldots,e_n)}$.*

Выше было показано, что объемы всех невырожденных параллелепипедов под действием оператора изменяются одинаково. Это доказывает корректность данного определения.

Remark 5 *Из определения следует, что определитель определитель линейного оператора $a \in \mathrm{End}(V)$ равен определителю его матрицы в некотором базисе, т.е.* $\det a = \det a_e^e$.

1.8.4 Свойства определителя

(см. [1, стр 42])

Предложение 9 *Пусть $a, b \in \mathrm{End}(V), A, B \in \mathrm{Mat}(n, K)$, тогда*

1. $\det(a \circ b) = \det a \cdot \det b$, $\det(AB) = \det A \cdot \det B$.
2. $\mathrm{GL}(V) = \{a \in \mathrm{End}(V) | \det a \neq 0\}$, $\mathrm{GL}(n, K) = \{A \in \mathrm{Mat}(n, K) | \det A \neq 0\}$;
3. $\det : \mathrm{GL}(V) \longrightarrow K^*$ — *гомоморфизм мультипликативных групп.*
4. $\det : \mathrm{GL}(n, K) \longrightarrow K^*$ — *гомоморфизм мультипликативных групп.*

Доказательство.

1. Пусть e — базис пространства V. Предположим, что оператор b обратим, тогда в силу леммы 10 векторы $b(e_1), \ldots, b(e_n)$ образуют базис пространства V. Тогда

$$\det(a \circ b) = \frac{\omega(a(b((e_1)), \ldots, a(b(e_n)))}{\omega(e_1, \ldots, e_n)} = \\ = \frac{\omega(a(b((e_1)), \ldots, a(b(e_n)))\omega(b(e_1), \ldots, b(e_n))}{\omega(e_1, \ldots, e_n)\omega(b(e_1), \ldots, b(e_n))} = \det a \cdot \det b.$$

   Пусть теперь оператор b необратим. Тогда векторы $b(e_1), \ldots, b(e_n)$ линейно зависимы, а значит таковы и $a(b(e_1)), \ldots, a(b(e_n))$, поэтому в силу теоремы о формах объема $\omega(b(e_1), \ldots, b(e_n) = 0$ и $\omega(a(b(e_1)), \ldots, a(b(e_n)) = 0$. Последнее означает, что $\det a \circ b = 0 = \det b = \det a \cdot \det b$.

   Утверждение про матрицы следует из замечания 5.

2. уже было доказано в теореме о формах объема.

   Оставшиеся пункты лишь переформулировка уже доказанного.

Отметим очевидные, но очень важные для практики свойства определителя.

Предложение 10 *(см. [1, Предложение 3.3])*

1. $\det A = \det A^T$.
2. *Определитель матрицы с нулевым столбцом (строкой) равен нулю.*

3. *Значение определителя не меняется если одной строке(столбцу) матрицы прибавить другую, умноженную на число.*

4. *Определитель матрицы, в которой есть два пропорциональных столбца (строки), равен нулю.*

5. $\det(A_1, \ldots, \alpha A_i, \ldots, A_n) = \alpha \det(A_1, \ldots, A_i, \ldots, A_n)$;

Доказательство. Все утверждения являются следствием полилинейноности и антисимметричности определителя.

1.8.5 Определитель блочной матрицы

Предложение 11 *Определитель блочно-треугольной матрицы равен произведению определителей диагональных блоков. Т.е.*

$$\det \begin{pmatrix} A & * \\ 0 & B \end{pmatrix} = \det A \det B.$$

Доказательство. (см. [1, Предложение 3.4]). Пусть сначала $A = \det \begin{pmatrix} E & * \\ 0 & E \end{pmatrix}$. С помощью элементарных преобразований легко показать, что $\det A = 1$. Рассмотрим теперь n-форму ω на K^n:

$$\omega(B) = \det \begin{pmatrix} B & * \\ 0 & E \end{pmatrix}.$$

Нетрудно убедиться, что ω — форма объема, а значит (т.к. пространство форм объема одномерно) $\omega(B) = c \det B$ для некоторого $c \in K$. Подставим $B = E$, получим уже рассмотренный случай, тогда $1 = \omega(E) = c$, а значит $c = 1$ и, таким образом, $\det \begin{pmatrix} B & * \\ 0 & E \end{pmatrix} = \omega(B) = \det B$.

Зафиксируем теперь квадратную матрицу B и рассмотрим m-форму u на K^m, заданную формулой $u(C) = \det \begin{pmatrix} B & * \\ 0 & C \end{pmatrix}$, где $C \in \mathrm{Mat}(m, K)$. Снова заметим, что u — форма объема, а значит $u(C) = d \det C$ для некоторого $d \in K$. Как и выше, подставив $C = E$, убедимся, что $d = \det B$, откуда следует утверждение. Общий случай(случай нескольких блоков) может быть получен по индукции. □

1.8.6 Разложение определителя по столбцу (строке).

Определение 23 *Пусть $B \in \mathrm{Mat}(n, K)$ и $1 \leqslant i, j \leqslant n$. Минором в позиции (i, j) матрицы B называется определитель матрицы, полученной из B вычеркиванием i-й строки и j-го столбца. Обозначим его $M_{ij}(B)$.*

Алгебраическим дополнением позиции (i,j) *матрицы* A *называется* $A_{ij} = (-1)^{i+j} M_{ij}(B)$.

Минор матрицы M^{ij}. *Алгебраическое дополнение.*

Предложение 12 *Пусть* $B \in \mathrm{Mat}(n,K)$. *Тогда*

$$\det B = \sum_{i=1}^{n} b_j^i A_{ij} = \sum_{i=1}^{n} b_i^j A_{ji}.$$

1.9 Матрицы. Часть 2.

1.9.1 Обратная матрица. Формулы Крамера.

(см.[стр.44] [1]) Обратимые матрицы.Решение систем методом Крамера.

Определение 24 *Пусть* $B \in \mathrm{Mat}(n,K)$. *Присоединенной к* B *называется матрица* $\mathrm{Adj}(B)$, *транспонированная к матрице из алгебраических дополнений матрицы* B.

Теорема 13 *Пусть* $A \in \mathrm{Mat}(n,K)$, *тогда*

$$A\mathrm{Adj}(A) = \mathrm{Adj}(A)A = (\det A)E.$$

В частности, если A *обратима, то* $A^{-1} = \frac{1}{\det A}\mathrm{Adj}(A)$.

Теорема 14 *(формулы Крамера). Пусть* $A \in \mathrm{Mat}(n,K)$, $b \in K^n$, *тогда система линейных уравнений* $Ax = b$ *имеет единственное решение тогда и только тогда, когда* $\Delta := \det A \neq 0$, *причем в случае* $\Delta \neq 0$, *решение системы имеет вид* $x_i = \frac{\Delta_i}{\Delta}$, $1 \leqslant i \leqslant n$, *где* Δ_i — *определитель матрицы, полученной из* A *заменой* i*-го столбца столбцом* b.

1.9.2 Минорный ранг матрицы.

(см.[стр.45] [1])

Теорема 15 *Ранг матрицы равен размеру наибольшей квадратной подматрицы, определитель, которой не равен нулю.*

Доказательство. (см. [1, Теорема 5.2]). Пусть $r = \mathrm{rk}\, A$, а $k \times k$ — размер наибольшей квадратной подматрицы, определитель, которой не равен нулю. Строки подматрицы размера $k \times k$ линейно независимы, а значит линейно независимы и соответствующие строки матрицы A. Таким образом $r \geqslant k$. Покажем, что $r \leqslant k$. У матрицы A найдутся r линейно независимых строк. Они образуют подматрицу ранга r, а значит в ней найдется r линейно независимых столбцов, которые образуют квадратную невырожденную матрицу ранга r. $\square$

1.9.3 Обратимые матрицы. Алгебра матриц. Матричные уравнения.

1.10 Двойственное пространство.

Пусть, как обычно, V — векторное пространство над полем K.

Определение 25 *Линейной функцией на V будем называть 1-форму, т.е. линейное отображение $V \longrightarrow K$.*

Линейную функцию естественно рассматривать как линейное отображение из пространство V в одномерное векторное пространство K. Поэтому всякая линейная функция однозначно задается значениями на базисных векторах и в случае, если пространство V конечномерно, матрица линейной функции является строкой.

Примеры.

1. Ясно, что всякая строка $u \in \mathrm{Mat}(1, n)$ задает линейное отображение $K^n \longrightarrow K$.
2. Пусть V — пространство функций $X \longrightarrow K$ и $x_0 \in X$. Тогда $f \mapsto f(x_0)$ является линейной функцией на пространстве V.
3. Пусть $e = (e_1, \ldots, e_n)$ — базис пространства V. Тогда

$$\begin{aligned} e^i : V &\longrightarrow K \\ x &\mapsto (x^e)^i, \end{aligned}$$

   где $1 \leqslant i \leqslant n$ — линейная функция. Функции ε будем называть координатными.

Определение 26 *Пространство линейных функций на V называется двойственным(сопряженным, дуальным) пространством по отношению к V и обозначается V^*.*

Элементы пространства V иногда называют ковекторами.

Теорема 16 *1. Пусть пространство V конечномерно. Тогда $\dim V = \dim V^*$. Причем, если $e = (e_1, \ldots, e_n)$ — базис пространства V, то функции $e^i, 1 \leqslant i \leqslant n$ образуют базис пространства V^*.*

Определение 27 *Базис $e^1, \ldots, e^n$ будем называть двойственным к базису $e = (e_1, \ldots, e_n)$.*

Пусть $v \in V$. Нетрудно проверить, что функция, определенная равенством $f_v(\alpha) = \alpha(v)$, где $\alpha \in V^*$ является линейной функцией на V^*, т.е. f_v лежит в пространстве V^{**}.

Теорема 17 *Пусть пространство V конечномерно. Отображение*

$$V \longrightarrow V^{**}$$
$$v \mapsto f_v$$

является каноническим изоморфизмом.

Remark 6 *Предположение конечномерности пространства существенно.*

1.10.1 Двойственное отображение.

Всякое линейное отображение $\varphi : U \longrightarrow V$ задает отображение $\varphi^* : V^* \longrightarrow U^*$ по формуле

$$\varphi^*(f) = f \circ \varphi.$$

Предложение 13 *Пусть e и f — базисы пространств U и V соответственно. $a : U \longrightarrow V$ — линейное отображение. Тогда*

$$(a_e^f)^T = (a^*)_{\widetilde{f}}^{\widetilde{e}},$$

где $\widetilde{e}, \widetilde{f}$ — двойственные базисы для e и f.

Corollary 4 $a^{**} = a$.

1.11

1.11.1 Инвариантные подпространства

Пусть U — подпространство V и $a \in \mathrm{End}(V)$. Образ подпространства U естественно обозначить через aU.

Определение 28 *Подпространство $U \leqslant V$ инвариантно относительно линейного оператора $a : V \longrightarrow V$, если $aU \subseteqq U$.*

Примеры.

1. $\mathrm{Ker}\, a$, $\mathrm{Im}\, a$.
2. $\frac{\partial}{\partial x} : K[x] \longrightarrow K[x]$. $K_n[x] = \{f \in K[x] | \deg f \leqslant n\}$ — инвариантное подпространство.

Remark 7 *Пусть U — инвариантное подпространство пространства V относительно оператора a. Тогда естественным образом определено сужение оператора a на пространство U. Пусть $e_1, \ldots, e_m$ — базис U. Дополним его до базиса $e_1, \ldots, e_m, e_{m+1}, \ldots, e_n$ пространства V. В построенном базисе матрица оператора a имеет вид*

$$\begin{pmatrix} A_1 & * \\ 0 & * \end{pmatrix},$$

где $A_1 \in \mathrm{Mat}(m, K)$ — матрица оператора $a|_U$.

Теорема 18 *Пусть $a \in \mathrm{End}(V)$. Тогда V раскладывается в прямую сумму двух инвариантных подпространств (т.е. существуют такие инвариантные подпротранства $U, W \leqslant V$, что $V = U \oplus W$) тогда и только тогда, когда существует базис e пространства V, такой что матрица a_e имеет вид*

$$a_e = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}.$$

Corollary 5 *Пусть $a \in \mathrm{End}(V)$. Тогда V раскладывается в прямую сумму m инвариантных подпространств (т.е. $V = U_1 \oplus \ldots \oplus U_n$) тогда и только тогда, когда существует базис e пространства V, такой что матрица a_e имеет блочно-диагональный вид.*

1.11.2 Многочлены от операторов. Минимальный многочлен оператора.

Определение 29 *Пусть V — векторное пространство над полем K и, одновременно, кольцо с той же операцией сложения. Если выполнено $\alpha(ab) = (\alpha a)b = a(\alpha b)$, $\forall a, b \in V, \alpha \in K$, то V называется алгеброй над полем K.*

Примеры.$\mathrm{End}(V)$

Определение 30 *Пусть V — векторное пространство, $a \in \mathrm{End}(V)$ и $f(x) = f_0 + f_1 x + \ldots + f_n x^n \in K[x]$. Положим*

$$f(a) = f_0 \,\mathrm{id} + f_1 a + \ldots + f_n a^n.$$

Remark 8 $a^n = a \circ a \circ \ldots \circ a$.

Тем самым определили гомоморфизм алгебр

$$\begin{aligned} K[x] &\longrightarrow \mathrm{End}(V) \\ f &\mapsto f(a). \end{aligned}$$

Как уже известно, ядро этого гомоморфизма является идеалом кольца $K[x]$, а в кольце $K[x]$ все идеалы главные. Таким образом, получили

$$I = \{f \in K[x] | f(a) = 0\} = \mu_a(x)K[x].$$

Среди многочленов, порождающих идеал I есть (причем единственный), старший коэффициент которого равен 1. Его будем называть минимальным многочленом оператора a.

Определение 31 *Многочлен $\mu \in K[X]$ называется минимальным многочленом оператора a, если $\deg \mu = \min\{\deg f | f(a) = 0\}$ и старший коэффициент μ равен единице.*

Рассуждения выше показывают существование и единственность минимального многочлена оператора.

1.11.3 О ядрах многочлена от оператора

Лемма 19 *1. Пусть $f(x) \in K[x]$, тогда $a(\operatorname{Ker} f(a)) \subseteq \operatorname{Ker} f(a)$.*

2. Если $f, g \in K[x]$ и $f|g$, то $\operatorname{Ker} f(a) \subseteq \operatorname{Ker} g(a)$.

Доказательство.

1. Пусть $v \in \operatorname{Ker} f(a)$, покажем, что $a(v) \in \operatorname{Ker} f(a)$. Действительно, $f(a)(a(v)) = (xf(x))(a)(v) = a(f(a)(v)) = a(0) = 0$.
2. $f|g \Longrightarrow g = hf \Longrightarrow g(a) = h(a) \circ f(a) \Longrightarrow \operatorname{Ker} f(a) \subseteq \operatorname{Ker} g(a)$.

Предложение 14 *Пусть многочлены $f_1, \ldots, f_k$ попарно взаимно просты. Тогда*

$$\operatorname{Ker}(f_1 \ldots f_k)(a) = \operatorname{Ker} f_1(a) \oplus \ldots \oplus \operatorname{Ker} f_k(a).$$

Доказательство. Докажем утверждение для случая $k = 2$, общий случай может быть получен индукцией по k. Многочлены f_1 и f_2 взаимно просты, следовательно найдутся многочлены g_1 и g_2 такие, что $1 = f_1 g_1 + f_2 g_2$, тогда

$$\mathrm{id} = g_1(a) \circ f_1(a) + g_2(a) \circ f_2(a). \tag{7}$$

Рассмотрим $v \in \operatorname{Ker}(f_1 f_2(a))$. Из (7) следует, что

$$v = g_1(a) \circ f_1(a)(v) + g_2(a) \circ f_2(a)(v). \tag{8}$$

Покажем, что $g_1(a) \circ f_1(a)(v) \in \operatorname{Ker} f_2(a)$. $v \in \operatorname{Ker}(f_1 f_2(a))$, поэтому $f_1(a)(v) \in \operatorname{Ker}(f_2(a))$. Пусть $g_1(x) = \beta_0 + \beta_1 x + \ldots + \beta_m x^m$, тогда

$$g_1(a) \circ f_1(a)(v) = \beta_0 \cdot f_1(a)(v) + \beta_1 a(f_1(a)(v)) + \ldots + \beta_m a^m(f_1(a(v))).$$

По лемме, каждое слагаемое этой суммы лежит в $\operatorname{Ker} f_2(a)(v)$, а значит и $g_1(a) \circ f_1(a)(v) \in \operatorname{Ker} f_2(a)$.

Аналогично $g_2(a) \circ f_2(a)(v) \in \operatorname{Ker} f_1(a)$.

Осталось показать, что $\operatorname{Ker} f_1(a) \cap \operatorname{Ker} f_2(a) = \{0\}$. Если $v \in \operatorname{Ker} f_1(a) \cap \operatorname{Ker} f_2(a)$, то, в силу (8) $v = 0$. $\square$

1.11.4 Проекторы

Проектор (идемпотент): $a^2 = a \Leftrightarrow V = \operatorname{Ker}(a - \mathrm{id}_V) \oplus \operatorname{Ker} a$. Отражение: $a^2 = \mathrm{id}_V \Leftrightarrow V = \operatorname{Ker}(a - \mathrm{id}_V) \oplus \operatorname{Ker}(a + \mathrm{id}_V)$ (здесь $\operatorname{char} K \neq 2$).

1.11.5 След линейного оператора

Определение 32 • *Следом матрицы* $A \in \operatorname{Mat}(n, K)$ *называется выражение* $\operatorname{tr} A = \sum_{i=1}^{n} A_i^i$.

• *След линейного оператора* a $\operatorname{tr} a = \operatorname{tr} a_e^e$.

Remark 9 *След оператора определен корректно, т.е. не зависит от выбора базиса.*

Действительно, проверим, для начала, что для $A, B \in \operatorname{Mat}(n, K)$ выполнено

$$\operatorname{tr} AB = \operatorname{tr} BA.$$

Из последнего равенства следует, что $\operatorname{tr} a_e^e = \operatorname{tr} C_f^e C_e^f a_e^e = \operatorname{tr} C_e^f a_e^e C_f^e = \operatorname{tr} a_f^f$.

Предложение 15 *Функция* $\operatorname{tr} : \operatorname{End}(V) \longrightarrow K$ *линейна, т.е.*

$$\operatorname{tr}(\alpha a + \beta b) = \alpha \operatorname{tr} a + \beta \operatorname{tr} b.$$

1.12 Спектр оператора и характеристический многочлен оператора

Пусть $a \in \operatorname{End}(V)$.

Определение 33 *Ненулевой вектор* $v \in V$ *называется собственным вектором оператора* a*, если* $av = \lambda v$*. Скаляр* $\lambda \in K$ *называется собственным значением оператора* a*, отвечающим собственному вектору* v*.*

Таким образом собственным является любой ненулевой вектор одномерного инвариантного подпространства.

Примеры.

собственные векторы оператора дифференцирования на пространстве многочленов.

Далее почти всегда будем предполагать, что пространство V конечномерно.

Предложение 16 *Число λ является собственным числом оператора $a \in \mathrm{End}(V)$ тогда и только тогда, когда $\det(a - \lambda \cdot \mathrm{id}) = 0$.*

Доказательство. Условие $av = \lambda v$ эквивалентно тому, что $\mathrm{Ker}(a - \lambda \cdot \mathrm{id}) \neq \{0\}$, что означает необратимость оператора $a - \lambda \cdot \mathrm{id}$, что равносильно тому, что $\det(a - \lambda \cdot \mathrm{id}) = 0$. □

$\mathrm{Spec}(a) = \{c \in K \mid (a - c \cdot \mathrm{id}_V) \notin \mathrm{GL}(V)\}$.

Определение 34 *Характеристическим многочленом матрицы A называется $\chi_A(t) = \det(t \cdot E - A)$.*

Характеристическим многочленом оператора назовем характеристический многочлен его матрицы в произвольном базисе.

Remark 10 *Характеристическим многочленом оператора определен корректно, т.е. не зависит от выбора базиса.*

Действительно,

$$\chi_{a_e}(t) = \det(t \cdot E - a_e) = \det(t \cdot E - C_f^e a_f C_e^f) = \det C_f^e (t \cdot E - a_f) C_e^f = \chi_{a_f}(t).$$

Легко видеть, что если $n = \dim V$, то $\chi_A(t) = t^n + \dots$.

Предложение 17 *1. Собственные числа (оператора/матрицы) и только они являются корнями характеристического многочлена (оператора/матрицы).*

2. *Пусть e и f — базисы пространства V. Тогда $\chi_{a_e}(t) = \chi_{a_f}$, $\mathrm{Spec}\, a_e = \mathrm{Spec}\, a_f = \mathrm{Spec}\, a$.*
3. $\chi_a(t) = t^n - \mathrm{tr}\, a \cdot t^{n-1} + \ldots + (-1)^n \det a$.

Доказательство. Первое утверждение следует из предложения **??**. Второе и третье уже доказаны. □

Corollary 6 *Если $K = \mathbb{C}$, то любой линейный оператор имеет собственный вектор. (Здесь важно, что пространство конечномерное.)*

Теорема Гамильтона-Кэли. Кратности собственных чисел.

Теорема 19 *Теорема Гамильтона-Кэли.*

Пусть V — векторное пространство над полем K ,$\dim V < \infty$ и $a \in \mathrm{End}(V)$. Тогда $\chi_a(a) = 0$.

Доказательство. Пусть A — матрица оператора A в каком-нибудь базисе. Достаточно доказать, что $\chi_A(A) = 0$. Пусть $\chi_A(t) = t^n + c_{n-1}t^{n-1} + \ldots + c_0$.

Обозначим

$$B := \mathrm{Adj}(t \cdot E - A).$$

(Вообще говоря мы рассматриваем объект из $\mathrm{Mat}(n, K[t])$, т.е. из кольца матриц над кольцом многочленов. Раннее мы рассматривали только матрицы над полем.) Тогда $(t \cdot E - A) \cdot B = \det(t \cdot E - A)E = \chi_A(t)E$. Представим матрицу B в виде $B = \sum_{i=0}^{n-1} t^i B_i$. Тогда

$$\chi_A(t) \cdot E = (t \cdot E - A)B = (t \cdot E - A)\sum_{i=0}^{n-1} t^i B_i = \sum_{i=0}^{n-1} t \cdot E \cdot t^i B_i - \sum_{i=0}^{n-1} t^i AB_i =$$
$$= \sum_{i=0}^{n-1} \cdot t^{i+1} B_i - \sum_{i=0}^{n-1} t^i AB_i = t^n B_{n-1} + \sum_{i=1}^{n-1} t^i (B_{i-1} - AB_i) - AB_0.$$

А значит,

$$B_{n-1} = E,$$
$$B_{i-1} - AB_i = c_i E,\ 1 \leqslant i \leqslant n-1$$
$$-AB_0 = c_0 E.$$

Таким образом

$$\chi_A(A) = A^n + c_{n-1}A^{n-1} + \ldots + c_0 =$$
$$= A^n + (B_{n-2} - AB_{n-1})A^{n-1} + (B_{n-3} - AB_{n-2})A^{n-2} + \ldots + (B_0 - AB_1)A - AB_0 = 0.$$

□

Corollary 7 *1. Минимальный многочлен оператора делит характеристический.*

2. Собственные числа и только они являются корнями минимального многочлена.

Доказательство. Первое утверждение следует из теоремы. Т.к. минимальный многочлен делит характеристический, то все корни минимального многочлена являются корнями характеристического. Обратно, пусть $\mu(x) = \sum_{i=0}^{m} c_i x^i$ — минимальный многочлен оператора, и λ — собственное число оператора a, т.е. найдется $v \neq 0$ такой, что $av = \lambda v$. Тогда $0 = \mu(a)(v) = \sum_{i=0}^{m} c_i \lambda^i v = \mu(\lambda)(v)$, а значит $\mu(\lambda) = 0$.

кратности собственных чисел

Определение 35 *Собственным подпространством, соответствующим собственному числу λ называется ядро оператора $a - \lambda \mathrm{id}$.*

Определение 36 • *Алгебраической кратностью $\alpha(a, \lambda)$ собственного числа называется его кратность в характеристическом многочлене.*

• *Геометрической кратностью собственного числа называется размерность его собственного подпространства.*

Лемма 20 *Геометрическая кратность $\gamma(a, \lambda)$ собственного числа не превосходит его алгебраической кратности.*

Доказательство. Выберем базис собственного пространства, соответствующего собственному числу λ и дополним его до базиса всего пространства. Матрица оператора a в рассматриваемом базисе имеет вид

$$\begin{pmatrix} \lambda E_\gamma & * \\ 0 & * \end{pmatrix}.$$

А значит, χ_a делится на $(x - \lambda)^\gamma$.

1.13 Собственные значения и корневые подпространства линейного оператора.

Теорема 20 *1. Сумма собственных подпространств прямая.*

2. Собственные вектора, соответствующие различным собственным числам линейно независимы.

Доказательство. Убедимся, что утверждение теоремы является следствием предложения 14. Пусть $v_1, \ldots, v_k$ — собственные векторы, соответствующие различным собственным значениям $\lambda_1, \ldots, \lambda_k$. Это означает, что $v_i \neq 0$ и $v_i \in \mathrm{Ker}(x - \lambda_i)(a)$ при всех $1 \leqslant i \leqslant n$. Т.к. λ_i попарно различны, то многочлены $f_i(x) = x - \lambda_i$ попарно взаимно просты, а значит (в силу предложения 14)

$$\mathrm{Ker}(f_1 \ldots f_k)(a) = \oplus \mathrm{Ker}\, f_i(a).$$

1.14 Диагонализуемость линейного оператора.

Определение 37 *Назовем оператор $a \in \mathrm{End}(V)$ диагонализуемым(диагонализируемым), если существует базис пространства V, в котором матрица оператора a диагональна.*

Теорема 21 *V — векторное пространство над полем K , $\dim V < \infty$ и $a \in \mathrm{End}(V)$; тогда следующие утверждения эквивалентны:*

1. *существует такой базис e, что a_e^e — диагональная матрица;*
2. $\mu_a = \prod_{c\in\mathrm{Spec}(a)}(x-c)$ *(то есть многочлен μ_a раскладывается без кратностей в произведение многочленов степени 1 в кольце $K[x]$);*
3. *Пространство V раскладывается в прямую сумму собственных подпространств линейного оператора a;*
4. $\dim V = \sum_{c\in\mathrm{Spec}(a)} \gamma(a,c)$.

Доказательство.

- $1 \Longrightarrow 2$. Существует базис оператора a состоящий из собственных векторов. Раннее было показано, что всякое собственное значение является корнем минимального многочлена, поэтому $\prod_{\lambda\in\mathrm{Spec}(a)}(x-\lambda)|\mu_a$. Остается показать, что $\prod_{\lambda\in\mathrm{Spec}(a)}(x-\lambda)(a) = 0$. Для этого достаточно показать, что $\prod_{\lambda\in\mathrm{Spec}(a)}(x-\lambda)(a)(v) = 0$ для всякого базисного вектора v. Рассмотрим базис из собственных векторов (который существует в силу предположения). Тогда для каждого базисного вектора v_i выполнено $(x-\lambda_i)(a)(v_i) = 0$ для соответствующего собственного числа λ_i, откуда следует требуемое.
- $2 \Longrightarrow 3$ В силу предложения 14
$$V = \mathrm{Ker}(\mu_a(a)) = \mathrm{Ker}\prod_{\lambda\in\mathrm{Spec}(a)}(x-\lambda)(a) = \bigoplus \mathrm{Ker}_{\lambda\in\mathrm{Spec}(a)}(x-\lambda)(a).$$
- $3 \Longrightarrow 4$
$$\dim V = \dim \bigoplus_{\lambda\in\mathrm{Spec}(a)} \mathrm{Ker}(x-\lambda)(a) = \sum_{\lambda\in\mathrm{Spec}(a)} \dim \mathrm{Ker}(x-\lambda)(a) = \\ = \sum_{\lambda\in\mathrm{Spec}(a)} \gamma(a,\lambda).$$
- $4 \Longrightarrow 1$ Так как сумма собственных подпространств прямая, то в силу совпадения размерностей, пространство V раскладывается в прямую сумму собственных подпространств. Рассмотрим объединение базисов собственных подпространств, получим искомый базис.

□

1.15 Жорданова форма линейного оператора.

1.15.1 Корневые подпространства. Пространства $\mathrm{Ker}(a-\lambda\,\mathrm{id})^j$.

V — конечномерное векторное пространство над полем K, $a \in \mathrm{End}(V)$.

Определение 38 *Вектор $v \in V$ называется корневым вектором оператора a, отвечающим числу $\lambda \in K$, если*

$$(a - \lambda \cdot \mathrm{id})^m v = 0$$

для некоторого $m \in \mathbb{N}$. Наименьшее такое m называется высотой вектора v.

Таким образом собственные векторы — корневые векторы, высоты 1. Корневые векторы, отвечающие числу $\lambda \in K$, образуют подпространство, которое обозначим $V^\lambda(a) = \bigcup_j \mathrm{Ker}(a - \lambda\,\mathrm{id})^j$.

Лемма 21 *1. $V^\lambda(a)$ инвариантно относительно оператора a.*

2. $\mathrm{Ker}(a - \lambda\,\mathrm{id})^j \subseteq \mathrm{Ker}(a - \lambda\,\mathrm{id})^{j+1}$.

3. Если $\mathrm{Ker}(a - \lambda\,\mathrm{id})^j = \mathrm{Ker}(a - \lambda\,\mathrm{id})^{j+1}$, *то* $\mathrm{Ker}(a - \lambda\,\mathrm{id})^{j+1} = \mathrm{Ker}(a - \lambda\,\mathrm{id})^{j+2} = \ldots \mathrm{Ker}(a - \lambda\,\mathrm{id})^m$, $\forall m \geqslant j$.

Доказательство.

1. $V^\lambda(a)$ инвариантно относительно оператора $a - \lambda\,\mathrm{id}$, а значит и относительно a. ($av = (a - \lambda \cdot \mathrm{id})v + \lambda v$.)
2. $\mathrm{Ker}(a - \lambda\,\mathrm{id})^j \subseteq \mathrm{Ker}(a - \lambda\,\mathrm{id})^{j+1}$.
3. ПустьKer$(a - \lambda\,\mathrm{id})^j = \mathrm{Ker}(a - \lambda\,\mathrm{id})^{j+1}$, тогда если $\mathrm{Ker}(a - \lambda\,\mathrm{id})^{j+1} \neq \mathrm{Ker}(a - \lambda\,\mathrm{id})^{j+2}$, то найдется вектор $v \in \mathrm{Ker}(a - \lambda\,\mathrm{id})^{j+2} \setminus \mathrm{Ker}(a - \lambda\,\mathrm{id})^{j+1}$. Тогда

$$(a - \lambda\,\mathrm{id})(v) \in \mathrm{Ker}(a - \lambda\,\mathrm{id})^{j+1} \setminus \mathrm{Ker}(a - \lambda\,\mathrm{id})^j,$$

что противоречит предположению.

□

Таким образом $V^\lambda(a) = \mathrm{Ker}(a - \lambda\,\mathrm{id})^m$ для некоторого m.

Теорема 22 *(Теорема о разложении в прямую сумму корневых подпространств.)*

Пусть $\dim V < \infty$, $a \in \mathrm{End}(V)$ *и многочлен χ_a раскладывается в произведение многочленов степени 1 в кольце $K[x]$. Тогда $V = \bigoplus_{\lambda \in \mathrm{Spec}(a)} V^\lambda(a)$ (то есть пространство V раскладывается в прямую сумму корневых подпространств линейного оператора a);*

(если $K = \mathbb{C}$, то это условие выполнено для любых $a \in \mathrm{End}(V)$ в силу алгебраической замкнутости поля$\mathbb{C}$);

Доказательство. $V = \mathrm{Ker}\,\chi_a(a) = \bigoplus \mathrm{Ker}(a - \lambda\,\mathrm{id})^{\alpha(a,\lambda)}$.□

Remark 11 *Сужение оператора $a - \lambda\,\mathrm{id}$ на подпространство* $\mathrm{Ker}(a - \lambda\,\mathrm{id})^j$ *— нильпотентный оператор.*

1.15.2 Жорданов базис. Случай нильпотентного оператора.

Пусть b — нильпотентный оператор, т.е. $b^m = 0$ для некоторого m.

Определение 39 *Высота вектора $v \in V$*

$$\mathrm{ht} v = \min\{n : b^n v = 0\}.$$

Лемма 22 *Если $\mathrm{ht} v = h$, то векторы $v, bv, \ldots, b^{h-1}v$ линейно независимы.*

Доказательство. Пусть $\alpha_0 v + \alpha_1 bv + \ldots + \alpha_{h-1} b^{h-1} v = 0$. Пусть k — номер первого ненулевого коэффициента, т.е. $\alpha_j = 0$, $\forall j < k$. Применим к обеим частям равенства оператор b^{h-k-1}, получим

$$\alpha_k b^{h-1} v = 0,$$

что означает $\alpha_k = 0$. $\square$

Определение 40 *Пространство $\langle v, bv, \ldots, b^{h-1}v\rangle$ называется циклическим подпространством нильпотентного оператора N, порожденным вектором v.*

Лемма 23 *1. циклическое подпространство инвариантно относительно оператора b.*

2. Матрица ограничения оператора b на инвариантное подпространство $\langle v, bv, \ldots, b^{h-1}v\rangle$ в базисе $b^{h-1}v, \ldots, bv, v$ имеет вид

$$\begin{pmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ 0 & 0 & 0 & \ldots & 0 & 0 \end{pmatrix}.$$

3. Если U — циклическое инвариантное подпространство и $v \in U \setminus bU$, то U циклическое подпространство оператора b, порожденным вектором v.

4. Если U — циклическое инвариантное подпространство $\langle v, bv, \ldots, b^{h-1}v\rangle$, то $\mathrm{Ker}\, b|_U = \langle b^{h-1}v\rangle$.

Доказательство. Ясно, что $b(b^k v) = b^{k+1} v \in \langle v, bv, \ldots, b^{h-1}v\rangle$. $\square$

Теорема 23 *Пространство V раскладывается в прямую сумму циклических подпространств нильпотентного оператора N. Количество слагаемых равно* $\dim \mathrm{Ker}\, N$.

1.15.3 Относительные базисы.

Определение 41 *Пусть U — подпространство пространства V. Векторы $v_1, \ldots, v_k$ называются линейно независимыми относительно U, если никакая их нетривиальная линейная комбинация не лежит в U.*

Иными словами, $v_1, \ldots, v_k$ линейно независимы относительно U если из того, что $\alpha_1 v_1 + \ldots + \alpha_k v_k \in U$ следует, что все α_i равны нулю. Последнее эквивалентно тому, что образы векторов $v_1, \ldots, v_k$ при проекции $V \longrightarrow V/U$ будут линейно независимы.

Определение 42 *Пусть U — подпространство пространства V. Векторы $v_1, \ldots, v_k$ называются базисом V относительно U, если они линейно независимы относительно U и всякий вектор из V представляется в виде суммы линейной комбинации векторов $v_1, \ldots, v_k$ и вектора из U.*

Иными словами, набор векторов $v_1, \ldots, v_k$ является базисом V относительно U, если образы векторов $v_1, \ldots, v_k$ при проекции $V \longrightarrow V/U$ образуют базис V/U.

Лемма 24 *Если векторы $v_1, \ldots, v_s$ принадлежат $\operatorname{Ker} b^{j+1}$ и линейно независимы относительно подпространства $\operatorname{Ker} b^j$, то векторы $b(v_1), \ldots, b(v_s)$ принадлежат $\operatorname{Ker} b^j$ и линейно независимы относительно $\operatorname{Ker} b^{j-1}$.*

Доказательство. Пусть $\alpha_1 b v_1 + \ldots + \alpha_s b v_s \in \operatorname{Ker} b^{j-1}$, тогда $b^{j-1}(\alpha_1 b v_1 + \ldots + \alpha_s b v_s) = 0$, т.е.

$$b^j(\alpha_1 v_1 + \ldots + \alpha_s v_s) = 0.$$

А значит $\alpha_1 v_1 + \ldots + \alpha_s v_s \in \operatorname{Ker} b^j$, откуда $\alpha_i = 0, \forall 1 \leqslant i \leqslant s$. $\square$

1.15.4 Доказательство теоремы 23.

Доказательство теоремы 23. Рассмотрим базис $v_1, \ldots, v_s$ пространства $V = \operatorname{Ker} b^m$ относительно $\operatorname{Ker} b^{m-1}$. Дополним векторы $bv_1, \ldots, bv_s$ до базиса $\operatorname{Ker} b^{m-1}$ относительно $\operatorname{Ker} b^{m-2}$ и т.д.. Получим нужный базис пространства V.

Будем доказывать утверждение индукцией по $n = \dim V$. При $n = 1$ утверждение очевидно. Пусть $n > 1$. Пусть U — $n-1$-мерное подпространство, содержащее $\operatorname{Im} b$. Отметим, что U инвариантно, т.к. $bU \subseteq \operatorname{Im} N \subseteq U$.

По индукционному предположению

$$U = U_1 \oplus \ldots \oplus U_k,$$

где U_i — циклические инвариантные подпространства. Рассмотрим вектор $v \in V \setminus U$, тогда

$$bv = u_1 + \ldots + u_k,\ u_i \in U_i. \tag{9}$$

Если для некоторого i $u_i = bu_i' \in bU_i$, то заменим v на $v - u_i'$. В итоге получим, что для всех i либо $u_i = 0$ либо $u_i \notin bU_i$. Если теперь $bv = 0$, то $\langle v \rangle$ — инвариантное циклическое подпространство и

$$V = \langle v \rangle \oplus U_1 \oplus \ldots \oplus U_k.$$

Если $bv \neq 0$, то $\mathrm{ht} bv = \max \mathrm{ht} u_i$. Для определенности, путь $\mathrm{ht} bv = \mathrm{ht} u_1$. Тогда $\mathrm{ht} v = \mathrm{ht} u_1 + 1$. Проверим, что

$$V = \langle v, bv, \ldots, b^{\mathrm{htu}_1} v\rangle \oplus U_2 \oplus \ldots \oplus U_k.$$

Действительно, $u_1 \notin bU_1$, поэтому $\mathrm{ht} u_1 = \dim U_1$, а значит $\dim V = \mathrm{htu}_1 + 1 + \dim U_2 + \ldots + \dim U_k$. Осталось проверить, что

$$\langle v, bv, \ldots, b^{\mathrm{htu}_1} v\rangle \cap (U_2 \oplus \ldots \oplus U_k) = \emptyset.$$

Пусть $\alpha_0 v + \alpha_1 bv + \ldots + \alpha_{\mathrm{htu}_1} b^{\mathrm{htu}_1} v \in U_2 \oplus \ldots \oplus U_k$. $v \notin U$, поэтому $\alpha_0 = 0$. Далее, в силу (9)

$$\alpha_1 bv + \ldots + \alpha_{\mathrm{htu}_1} b^{\mathrm{htu}_1} v = \alpha_1 u_1 + \ldots + \alpha_{\mathrm{htu}_1} b^{\mathrm{htu}_1 - 1} u_1 + z,$$

где $z \in U_2 \oplus \ldots \oplus U_k$. Но $U_1 \cap (U_2 \oplus \ldots \oplus U_k) = \emptyset$, а значит $\alpha_1 u_1 + \ldots + \alpha_{\mathrm{htu}_1} b^{\mathrm{htu}_1 - 1} u_1 = 0$, откуда все α_i равны нулю. Докажем вторую часть теоремы. Пусть $V = V_1 \oplus \ldots \oplus V_k$ разложение в прямую сумму инвариантных циклических подпространств. Тогда $\operatorname{Ker} b = \operatorname{Ker} b|_{V_1} \oplus \ldots \oplus \operatorname{Ker} b|_{V_k}$. Но $\dim \operatorname{Ker} b|_{V_i} = 1$, поэтому $k = \dim \operatorname{Ker} b$. $\square$

1.15.5 Жорданов базис. Общий случай.

Пусть $a \in \mathrm{End}(V)$ — произвольный линейный оператор. Заметим, что оператор $b := (a - \lambda \mathrm{id})|_{V^\lambda(a)}$ нильпотентный. Пусть $U = \langle v, bv, \ldots, b^{h-1} v\rangle$ циклическое подпространство относительно оператора b. Тогда $a(b^k v) = a(b^k v) - \lambda b^k v + \lambda b^k v = b(b^k v) + \lambda b^k v = \lambda b^k v + b^{k+1} v$, поэтому в базисе $b^{h-1} v, \ldots, bv, v$ матрица оператора $a|_U$ имеет вид

$$\begin{pmatrix} \lambda & 1 & 0 & \ldots & 0 \\ 0 & \lambda & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & 0 & \ldots & \lambda \end{pmatrix}.$$

Определение 43 *Жордановой матрицей называется клеточно-диагональная матрица*

$$J = \begin{pmatrix} J_1 & 0 & \ldots & 0 \\ 0 & J_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & J_k \end{pmatrix},$$

в которой $J_i = \begin{pmatrix} \lambda & 1 & 0 & \ldots & 0 \\ 0 & \lambda & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & 0 & \ldots & \lambda \end{pmatrix}$ *— жордановы клетки.*

Теорема 24 *1. Если характеристический многочлен $\chi_a(t)$ оператора a раскладывается на линейные множители, то существует базис, в котором матрица оператора a жорданова.*

2. *Количество жордановых клеток не зависит от выбора жорданова базиса.*

3. *Сумма порядков жордановых клеток с собственным значением λ равна размерности соответствующего корневого подпространства, т.е. $\alpha(a, \lambda)$.*

1.15.6 К построению жорданова базиса

1. Минимальный многочлен жордановой клетки порядка m с собственным значением λ есть $(t - \lambda)^m$.

1.16 Функции от операторов.

1.16.1 Значение многочлена от матрицы

Сведем вычисление значения многочлена от оператора к вычислению значения многочлена степени, меньшей чем n от оператора.

$$f(x) = q(x)\chi_a(x) + r(x),\ \deg r < n.$$

Тогда $f(a) = r(a)$.

В случае, если χ_a раскладывается на линейные множители $\chi_a = \prod (x - \lambda_i)^{m_i}$, многочлен $r(x)$ однозначно задается условиями

$$f^{(k)}(\lambda_i) = r^{(k)}(\lambda_i),\ 1 \leqslant k \leqslant m_i. \tag{10}$$

Значение многочлена от жордановой клетки. Выше было показано, что в случае алгебраически замкнутого поля K всякую матрицу $A \in \mathrm{Mat}(n, K)$ можно представить в виде $A = C^{-1}JC$, где $C \in \mathrm{GL}(n, K)$, а J — жорданова матрица. Нетрудно убедиться в том, что для всякого многочлена $f(x) \in K[x]$ выполнено

$$f(A) = C^{-1}f(J)C.$$

Для вычисления $f(J)$ заметим, что

$$\begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & \lambda \end{pmatrix}^k = \begin{pmatrix} \lambda^k & k\lambda^{k-1} & k(k-1)\lambda^{k-2}/2! & \dots & \dots \\ 0 & \lambda^k & k\lambda^{k-1} & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \dots \\ 0 & 0 & 0 & \dots & \lambda^k \end{pmatrix}.$$

1.16.2 Норма вектора, норма оператора, сходимость

Из курса анализа уже известно понятие нормы. Нормой в пространстве V называется функция $||\cdot|| : V \longrightarrow \mathbb{R}$, обладающая свойствами

1. $||x|| > 0$ при $x \neq 0$;
2. $||\lambda x|| = |\lambda| \cdot ||x||$;
3. $||x + y|| \leqslant ||x|| + ||y||$.

Также уже известно, что нормированное пространство является является метрическим с метрикой $\rho(u, v) = ||u - v||$ и определено понятие сходимости последовательности в метрическом пространстве. К известным фактам можно отнести и следующие утверждения:

1. В пространстве $\mathbb{R}^n$ сходимость по норме и покоординатная сходимость эквивалентны.
2. В пространстве $\mathbb{R}^n$ все нормы эквивалентны.

В курсе анализа уже упоминалось понятие нормы оператора.

Определение 44 *Пусть U, V — нормированные векторные пространства, а $a : U \longrightarrow V$ линейное отображение. Положим*

$$||a|| := \sup_{||u||=1} a(u) = \sup_{u \neq 0} \frac{a(u)}{||u||}.$$

Remark 12 *В случае, если пространства U и V конечномерны (а мы будем рассматривать только такие случаи),*

$$||a|| = \max_{||u||=1} a(u) = \max_{u \neq 0} \frac{a(u)}{||u||} < \infty.$$

Например, рассмотрев стандартную норму в $\mathbb{R}^n$ можно показать, что для $a : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ выполнено $||a|| \leqslant \sqrt{\sum a_{ij}^2}$.

Теперь пространство линейных отображений $U \longrightarrow V$ можно рассматривать как нормированное векторное пространство.

Предложение 18

$$||ab|| \leqslant ||a|| \cdot ||b||.$$

Доказательство.

$$||ab|| = \max_{v \neq 0} \frac{||ab(v)||}{||v||} = \max_{b(v) \neq 0} \frac{||ab(v)||}{||b(v)||} \cdot \frac{||b(v)||}{||v||} \leqslant \max_{b(v) \neq 0} \frac{||ab(v)||}{||b(v)||} \cdot \max_{b(v) \neq 0} \frac{||b(v)||}{||v||} \leqslant$$
$$\leqslant \max_{b(v) \neq 0} \frac{||a(w)||}{||w||} \cdot \max_{v \neq 0} \frac{||b(v)||}{||v||} = ||a|| \cdot ||b||.$$

□

Предложение 19 *Пусть U, V — нормированные векторные пространства, а $a : U \longrightarrow V$ линейное отображение и $||a|| < R$. Пусть ряд $f(x) = \sum c_n x^n (c_n \in \mathbb{R})$ сходится при $|x| < R$. Тогда ряд*

$$f(a) = \sum_{n=0}^{\infty} c_n a^n$$

сходится.

Доказательство. $||c_n a^n|| \leqslant |c_n| \cdot ||a||^n$

Теорема 25 *Пусть K алгебраически замкнуто, $f(x) = \sum_{i=0}^{\infty} c_i x^i$ и многочлен $r(x)$ определен условиями (10). Тогда $f(a) = r(a)$.*

Доказательство. Пусть $f_m(x) = \sum_{i=0}^{m} c_i x^i$ и r_m — многочлен, удовлетворяющий условиям (10) для функции f_m. (т.е. $f_m = q_m \chi_a + r_m$). Тогда $f_m(a) = r_m(a)$. $\lim r_m = r$, а значит

$$f(a) = \lim f_m(a) = \lim r_m(a) = r(a).$$

□

1.16.3 Экспонента линейного оператора.

$\mathrm{e}^a = \sum_{k=0}^{\infty} \frac{1}{k!} a^k$.

Теорема 26 *Теорема о свойствах экспоненты.*

1. *Пусть V — банахово пространство и $a, b \in \mathrm{End}(V)$ и пусть $a \circ b = b \circ a$, тогда $e^{a+b} = \mathrm{e}^a \circ \mathrm{e}^b$, а также $\mathrm{e}^0 = \mathrm{id}_V$ и $\mathrm{e}^{-a} = (\mathrm{e}^a)^{-1}$.*
2. *Пустьn $\in \mathbb{N}_0$ и $a \in \mathrm{Mat}(n, \mathbb{C})$; тогда $\det \mathrm{e}^a = \mathrm{e}^{\mathrm{tr}\, a}$, $\mathrm{e}^{a^{\mathtt{T}}} = (\mathrm{e}^a)^{\mathtt{T}}$ и $\mathrm{e}^{\overline{a}^{\mathtt{T}}} = \left(\overline{\mathrm{e}^a}\right)^{\mathtt{T}}$.*

Доказательство.

$$e^{a+b} = \sum_{k=0}^{\infty} \frac{1}{k!} (a+b)^k = \sum_{k=0}^{\infty} \frac{1}{k!} \sum_{i=0}^{k} C_k^i a^i b^{k-i}$$

$$(\sum_{k=0}^{\infty} \frac{1}{k!} a^k)(\sum_{l=0}^{\infty} \frac{1}{l!} b^l) = \sum_{k,l=0}^{\infty} \frac{1}{k!l!} a^k b^l = \sum_{k,l=0}^{\infty} \frac{1}{(k+l)!} C_{k+l}^k a^k b^l$$

Остается воспользоваться тем, что сумма абсолютно сходящегося ряда не изменяется ни при какой перестановке его членов.

2 Кольцо многочленов.

2.1 Разложение многочленов на неприводимые множители. Лемма Гаусса. Критерий Эйзенштейна

Напомним, что если R — область целостности, то $R[x]$ тоже. Многочлен $f(x)$ называется неприводимым, если из равенства $f = gh$ следует, что g или h ассоциирован с f. В области целостности последнее означает, что f не раскладывается в произведение необратимых элементов.

Определение 45 *Пусть R — факториальное кольцо. Содержанием многочлена $a_0 + a_1X + \ldots + a_nX^n$ называется наибольший общий делитель всех его коэффициентов $d(f) = \gcd(a_i)$.*

Нетрудно проверить, что для $c \in R, f(X) \in R[X]$ выполнено $d(cf(X)) = cd(f)$.

Лемма 25 *(лемма Гаусса) Пусть R — факториальное кольцо, $f, g \in R[X]$. Тогда $d(fg) = d(f) \cdot d(g)$*

Равенство естественно следует понимать как ассоциированность.

Доказательство. Покажем сначала, что если $d(f) = d(g) = 1$, то $d(fg) = 1$. Пусть

$$f(X) = a_0 + a_1X + \ldots + a_nX^n;$$
$$g(X) = b_0 + b_1X + \ldots + b_mX^m.$$

Предположим, что $d(fg) \neq 1$, тогда найдется простой элемент $p \in R$ такой, что $p|d(fg)$. Пусть s, t наименьшие индексы, для которых $p \nmid a_s$, $p \nmid b_t$. Как и все коэффициенты многочлена fg, его коэффициент при X^{s+t} делится на p. Тогда

$$0 \equiv \sum_{i+j=s+t} a_ib_j \equiv a_sb_t \mod p,$$

а значит $p|a_sb_t$, что невозможно, так как p — простой и $p \nmid a_s, p \nmid b_t$.

Перейдем к общему случаю. $f = d(f)f_0$, $g = d(g)g_0$, где $d(f_0) = d(g_0) = 1$. Тогда $d(fg) = d(d(f)f_0d(g)g_0) = d(f)d(g)$. □

Corollary 8 *Если многочлен $f(x) \in \mathbb{Z}[x]$ неприводим над $\mathbb{Z}$, то он неприводим и над $\mathbb{Q}$.*

Доказательство. Пусть $f = gh$, $g, h \in \mathbb{Q}[X]$, тогда $af = bg_0h_0$, где $g_0, h_0 \in \mathbb{Z}[X]$, $d(g_0) = d(h_0) = 1$. Получаем $ad(f) = b$, а значит $af = ad(f)g_0h_0$, откуда $f = d(f)g_0h_0$.□

2.1.1 Критерий Эйзенштейна

Теорема 27 *Пусть* $f(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in \mathbb{Z}[X]$ *и пусть все коэффициенты* $a_0, \ldots, a_{n-1}$ *делятся на простое число* p*, но* a_0 *не делится на* p^2 *и* a_n *не делится на* p*. Тогда* $f(X)$ *неприводим над* $\mathbb{Q}$*.*

Доказательство.Пусть

$$f(X) = (\sum_{k=0}^{m} b_kX^k)(\sum_{l=0}^{s} c_lX^l),\ m, s > 0.$$

$p \mid a_0 = b_0c_0 \Longrightarrow p$ делит одно из b_0, c_0 и не делит второе. Пусть, для определенности $p \mid b_0$, $p \nmid c_0$. $\{i|p \nmid b_i\} \neq \emptyset$, т.к. иначе $p \mid a_n$. Пусть $i_0 = \min\{i|p \nmid b_i\}$, тогда

$$p \mid a_{i_0} = \sum_{j=0}^{i} b_jc_{i_0-j} \equiv b_ic_0 \mod p.$$

Противоречие. □

Неприводимые многочлены над полями Унитарных неприводимых многочленов над полем K бесконечно много. (Достаточно для неприводимых многочленов $p_1, \ldots, p_n$ рассмотреть многочлен $p_1 \cdots p_n + 1$.) Если поле K конечно, то многочленов фиксированной степени тоже конечное число. Таким образом над конечным полем существуют неприводимые унитарные многочлены сколь угодно большой степени.

2.2 Многочлены над конечным полем

2.2.1 Факты о конечных полях.

Предложение 20 *1. Пусть* F *— конечное поле, тогда* $|F| = p^m$*, где* p *— простое число, равное характеристике поля* F*.*

2. Если F *— поле из* q *элементов, то* $a^{q-1} = 1$*,* $\forall a \in F$*.*

2.3 Алгоритм Берлекампа разложения многочлена на множители.

Теорема 28 *Пусть* $f \in \mathbb{F}_p[x]$ *— многочлен положительной степени* n *со старшим коэффициентом 1.*

1. Если многочлен $h \in \mathbb{F}_p[x]$ *удовлетворяет соотношению* $h^p \equiv h \mod f$*, то*

$$f(x) = \prod_{a \in \mathbb{F}_p} (f(x), h(x) - a).$$

2. *Пусть $f = f_1 \dots f_k$, где f_i — попарно различные неприводимые многочлены со старшим коэффициентом 1. В таком случае многочлен h удовлетворяет соотношению $h^p \equiv h \mod f$ тогда и только тогда, когда $h(x) \equiv a_i \mod f_i$, где $a_i \in \mathbb{F}_p$. При этом каждому набору $(a_1, \dots, a_k)$ соответствует ровно один многочлен h, степень которого меньше степени многочлена f.*

Доказательство.

1. Обозначим $F(X) = \prod_{a \in \mathbb{F}_p} (f(x), h(x) - a)$. Многочлены $f(X) - a$ взаимно просты при различных $a \in \mathbb{F}_p$, поэтому $(f(X), h(X) - a)$ взаимно простые делители $f(X)$, а значит $F(X) \mid f(X)$.

   Обратно. В поле $\mathbb{F}_p$ выполнено $\prod_{a \in \mathbb{F}_p} (y - a) = y^p - a$, а значит $\prod_{a \in \mathbb{F}_p} (h(X) - a) = h^p - h \vdots f$. Тогда

$$F(X) = \prod_{a \in \mathbb{F}_p} (f(x), h(x) - a) = (f(X), \prod_{a \in \mathbb{F}_p} (h(x) - a) \vdots f(X).$$

2. То, что каждому набору $(a_1, \dots, a_k)$ соответствует ровно один многочлен h, степень которого меньше степени многочлена f следует из китайской теоремы об остатках.

   $\Longrightarrow \prod_{a \in \mathbb{F}_p} (h(X) - a) = h^p - h \vdots f \Longrightarrow \prod_{a \in \mathbb{F}_p} (h(X) - a) = h^p - h \vdots f_i, \forall i$. Но, т.к. $f(X) - a$ попарно взаимно просты при различных $a \in \mathbb{F}_p$, то $\forall i \exists a_i : f_i \mid h(x) - a_i$.

   $\Longleftarrow$ если $h(X) \equiv a_i \mod f_i$, то $h^p \equiv a_i^p = a_i \equiv h \mod f_i$, а значит $h^p \equiv h \mod p$.

2.3.1 Алгоритм.

Remark 13 *В условиях теоремы предполагалось, что у многочлена f нет кратных неприводимых сомножителей. Покажем, что от кратных сомножителей можно избавиться. Пусть $f = f_1^{n_1} \dots f_k^{n_k}$, где f_i — попарно различные неприводимые многочлены со старшим коэффициентом 1. Тогда*

$$d = (f, f') = \prod_{p \nmid n_i} f_i^{n_i - 1} \prod_{p \mid n_i} f_i^{n_i},$$

откуда $f = d \prod_{p \nmid n_i} f_i$. Таким образом $f = d \cdot \frac{f}{d}$ и остается разложить многочлен $\frac{f}{d}$, у которого нет кратных неприводимых сомножителей.

Заметим, что условие $h^p(X) \equiv h(X) \mod f(X)$, $\deg h < \deg f = n$ эквивалентно системе линейных уравнений над $\mathbb{F}_p$. Действительно, пусть

$$h(X) = t_0 + t_1 X + \dots + t_{n-1} X^{n-1},$$

тогда

$$h^p(X) = h(X^p) = t_0 + t_1 X^p + \ldots + t_{n-1} X^{p(n-1)}.$$

Пусть

$$X^{pj} = \sum_{i=1}^{n-1} q_{ij} X^i \mod f,\ 0 \leqslant j \leqslant n-1.$$

Тогда $h^p \equiv h \mod f$ эквивалентно системе уравнений

$$t_i = \sum_{j=0}^{n-1} q_{ij} t_j,\ i = 0..n-1. \tag{11}$$

С другой стороны, из теоремы следует, что пространство решений $h^p \equiv h \mod f$ изоморфно $\mathbb{F}_p^k$, где k — количество неприводимых сомножителей в разложении многочлена $f(X)$. Таким образом размерность пространства решений системы (11) равна k. Пусть $h_1 = 1, h_2, \ldots, h_k$ — базис пространства решений системы (11). Если $k = 1$, то f неприводим. Если $k > 1$, то по теореме $f(X) = \prod_{a \in \mathbb{F}_p} (f(X), h_2(X) - a)$, откуда можно найти некоторые неприводимые сомножители разложения f, если таким образом найдены не все сомножители (их получилось меньше чем k), то рассмотрим $(g_i(X), h_3(X) - a)$, где g_i — один из уже найденных сомножителей. И т.д. В итоге получим разложение многочлена f. Действительно, рассмотрим два набора $(a_1, a_2, \ldots), (a_2, a_1, \ldots) \in \mathbb{F}_p^k$ им соответствуют h и θ, причем $\theta - a_1$ не делится на f_1, т.к. $\theta \equiv a_2 \mod f_1$, а значит $(\theta(X) - a_1, f)$ делится на f_2, но не делится на f_1.

Пример неприводимого многочлена, приводимого по любому простому модулю. Многочлен $X^4 + 1$ неприводим над $\mathbb{Z}$, но приводим по любому простому модулю p.

2.4 Факториальность кольца многочленов над факториальным кольцом.

Лемма 26 *Пусть $f, g \in R[x]$, причем f и g примитивные и $cf(X) = dh(X)$ для $c, d \in R \setminus \{0\}$. Тогда d и c ассоциировнаы в R, а f и g ассоциированы в $R[X]$.*

Теорема 29 *Если кольцо R факториально, то и $R[X]$ факториально.*

2.5 Многочлены от многих переменных

Определим $R[X_1, \ldots, X_n]$ как $R[X_1, \ldots, X_n] = R[X_1][X_2] \ldots [X_n]$. Нетрудно проверить, что любой многочлен от переменных $X_1, \ldots, X_n$ имеет вид

$$f(x_1, \ldots, x_n) = \sum_{k_1, \ldots, k_n} a_{k_1 \ldots k_n} x_1^{k_1} \cdots x_n^{k_n},$$

где суммирование происходит по конечному набору мультииндексов.

Определение 46 *Многочлен $\sum_{k_1, \ldots, k_n} a_{k_1 \ldots k_n} x_1^{k_1} \cdots x_n^{k_n}$ называется однородным степени d, если $a_{k_1 \ldots k_n} = 0$ при $k_1 + \ldots + k_n \neq d$.*

Однородные многочлены степени d образуют конечномерное подпространство $R^{(d)}[x_1, \ldots, x_n]$ размерности C_{n+d-1}^d. А также

$$R[X_1, \ldots, X_n] = \bigoplus_{d \geqslant 0} R^{(d)}[x_1, \ldots, x_n].$$

Предложение 21 *Если поле K бесконечно, то разные многочлены определяют разные функции.*

2.5.1 Теорема Гильберта о нулях, о базисе, базисы Гребнера и их использование в компьютерной алгебре.

Теорема 30 *(Теорема Гильберта о базисе) Пусть в кольце R любой идеал конечнопорожден, тогда и в $R[x_1, \ldots, x_n]$ любой идеал конечнопорожден.*

Доказательство. Достаточно показать, что в $R[X]$ всякий идеал конечнопорожден. Общее утверждение можно доказать по индукции. Пусть $I \subsetneqq R[X]$ некоторый идеал кольца $R[X]$. Старшие коэффициенты (и 0) многочленов из I образуют идеал J в кольце R. По предположению идеал J конечнопорожден. Пусть $J = \langle a_1, \ldots, a_s \rangle$. Пусть, далее $f_1, \ldots, f_s$ — многочлены из идеала I, для которых $f_i(X) = a_i X^{m_i} + \ldots$. Пусть $n = \max \deg f_i(X)$.

Заметим, что любой многочлен $f(X) \in I$ можно представить в виде

$$f(X) = g(X) + \sum_{i=1}^{s} \lambda_i f_i(X),\ \lambda_i \in R, \deg g < n.$$

Действительно, пусть $f(X) = b_N x^N + \ldots + b_1 X + b_0$ и $N > n$, тогда $b_N \in J$, а значит $b_N = \sum_{i=1}^{s} \alpha_i a_i$, поэтому $\deg(f(X) - \sum_{i=1}^{s} \alpha_i X^{N-m_i} f_i) < \deg f(X)$.

Теперь остается показать, что найдется конечный набор многочленов такой, что любой многочлен степени меньшей чем n является линейной комбинацией многочленов из этого набора. Пусть J_{n-1} идеал кольца R, состоящий из коэффициентов многочленов степени не выше $n-1$ из идеала I. Тогда $J_{n-1} = \langle b_1^{(n-1)}, \ldots, b_{t_1}^{(n-1)} \rangle$. Коэффициентам $b_1^{(n-1)}, \ldots, b_{t_1}^{(n-1)}$ соответствуют многочлены $g_i^{(n-1)}(X) = b_i^{(n-1)} X^{n-1} + \ldots \in I$. Как и выше, можно получить, что $\forall f \in I, \deg f \leqslant n-1,\ f = \sum \beta_i g_i(X) + f_{n-2}$, где $\deg f_{n-2} \leqslant n-2$. Данную конструкцию можно повторить еще раз, в результате будет построена конечная система образующих идеала I.

□

Remark 14 *Кольца, в которых любой идеал конечнопорожден называются нетеровыми. Условие, что всякий идеал конечнопорожден эквивалентно тому, что любая возрастающая цепочка идеалов стабилизируется. Мы уже сталкивались с этим понятием, в частности, доказывали, что кольцо главных идеалов является нётеровым. Утверждение теоремы можно переформулировать следующим образом: если кольцо R — нетерово, то кольцо $R[X]$ тоже нётерово. Аналогичным образом, но несколько сложнее, можно показать, что кольцо рядов $R[[X]]$ тоже будет нётеровым.*

2.6 Базисы Гребнера

Определим старший член многочлена для многочлена от нескольких переменных. Каждый одночлен(моном) имеет вид $\alpha X_1^{k_1} \cdots X_n^{k_n}$. Ввердем лексикографический порядок на множестве мономов. Будем считать, что $(i_1, \ldots, i_n) > (j_1, \ldots, j_n)$ если для некоторого $1 \leqslant k \leqslant n$ выполнено $i_1 = j_1, i_2 = j_2, \ldots, i_{k-1} = j_{k-1}, i_k > j_k$. Мономы будем сравнивать по соответствующим мультииндексам. Старшим членом многочлена $f(x_1, \ldots, x_n)$ будем называть ненулевой моном $St(f)$ наибольшей степени.

Remark 15 *Старший член произведения многочленов равен произведению их старших членов.*

Пусть K — поле. В случае $n = 1$ любой идеал главный и чтобы выяснить лежит ли многочлен $g(x)$ в идеале $\langle f(x) \rangle$ достаточно поделить g на f с остатком. Поставим аналогичную задачу в кольце $K[X_1, \ldots, X_n]$.

Remark 16 *Если $St(f) \vdots St(h)$, то $f = h \cdot f_1 + f_2$, где $St(f_2) < St(f)$.*

Замечание позволяет для всякого многочлена f и набора многочленов $g_1, \ldots, g_t$ представить f в виде

$$f(X) = \sum_{i=1}^{t} h_i(X) g_i(X) + r(X),$$

где $St(r)$ не делится ни на один из старших членов g_i. Получившийся многочлен r будем называть редукцией f при помощи $g_1, \ldots, g_t$. В случае если $f(X) = \sum_{i=1}^{t} h_i(X) g_i(X) + r(X)$, где $St(r)$ не делится ни на один из старших членов g_i, многочлен r уместно называть остатком при делении f на $\langle g_1, \ldots, g_t >$. Однозначно ли определен этот остаток?

Определение 47 *Будем говорить, что многочлена $g_1, \ldots, g_t$ образуют базис Грёбнера идеала $I \lhd K[X_1, \ldots, X_n]$, если $\forall f \in I \setminus \{0\}$ выполнено $St(f) \vdots St(g_i)$ для некоторого i.*

Теорема 31 *Пусть $g_1, \ldots, g_t \in I \lhd K[X_1, \ldots, X_n]$. Следующие условия эквивалентны.*

1. *$g_1, \ldots, g_t$ образуют базис Грёбнера идеала I.*
2. *Всякий многочлен из идеала I редуцируется к нулю при помощи $g_1, \ldots, g_t$. (и, тем самым $g_1, \ldots, g_t$ порождают идеал I.)*
3. *$f \in I \Longleftrightarrow f = \sum h_i g_i$ и $St(f)$ равен старшему из $St(h_i)St(g_i)$.*
4. *Идеал $L(I)$, порожденный старшими членами элементов идеала I, порожден старшими членами g_i.*

Доказательство. $1 \Longrightarrow 2$ Пусть $f(X) = \sum_{i=1}^{t} h_i(X) g_i(X) + r(X)$, где $St(r)$ не делится ни на один из старших членов g_i. Но тогда $r \in I$ и по определению получаем $r = 0$.
$2 \Longrightarrow 3$ Если $f \in I$, то $f = \sum h_i g_i$, а $St(f)$ равен старшему из $St(h_i)St(g_i)$ по определению редукции.
$3 \Longrightarrow 4$ очевидно.
$4 \Longrightarrow 1$ Пусть $f = aX^\alpha + \ldots \in I$, тогда $aX^\alpha = \sum_i b_i X^{\beta_i} St(g_i)$. Тогда X^α делится на $St(g_i)$ при некотором i.$\square$

Теорема 32 *У любого ненулевого идеала в $K[X_1, \ldots, X_n]$ есть базис Грёбнера.*

Доказательство. Пусть $L(I)$ идеал, порожденный старшими момномами многочленов из I. Тогда любой $f \in L(I)$ имеет вид $f = \sum h_i X^{\alpha_i}$. Поэтому, всякий моном многочлена $f \in L(I)$ делится на некоторый моном, который

является $St(h)$ некоторого $h \in I$. По теореме Гильберта о базисе, идеал $L(I)$ конечно порожден, т.е. $L(I) = \langle f_1, \ldots, f_k \rangle$. Каждый моном каждого из f_i делится на свой $St(h)$, поэтому $L(I)$ порожден конечным числом мономов, которые являются старшими членами многочленов $g_j \in I$. Тогда по предыдущей теореме g_j образуют базис Грёбнера идеала I. $\square$

Теорема 33 *$g_1, \ldots, g_t$ образуют базис Грёбнера идеала I тогда и только тогда, когда остаток от деления любого многочлена f на $g_1, \ldots, g_t$ определен однозначно.*

2.6.1 Алгоритм Бухбергера

Для многочленов f и g положим

$$S(f,g) = \frac{X^\gamma}{St(f)} f - \frac{X^\gamma}{St(g)} g,$$

где X^γ — наименьшее общее кратное мономов $St(f)$ и $St(g)$.

Теорема 34 *(Теорема Бухбергера) Многочлены $g_1, \ldots, g_t$ образуют базис Грёбнера идеала $I = \langle g_1, \ldots, g_t \rangle$ тогда и только тогда, когда при всех $i \neq j$ многочлен $S(g_i, g_j)$ редуцируется к нулю по модулю $g_1, \ldots, g_t$.*

Лемма 27 *Пусть $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$ таковы,что $St(f_i) = St(f_j) = X^\alpha$. Тогда если $St(\sum \lambda_i f_i) < X^\alpha$, где $\lambda_i \in K$, то $\sum \lambda_i f_i = \sum_{i<j} \mu_{ij} S(f_i, f_j)$.*

Доказательство. Т.к. $f_i = a_i X^\alpha + \ldots$, то $S(f_i, f_j) = \frac{f_i}{a_i} - \frac{f_j}{a_j}$. Заметим, что

$$\sum \lambda_i f_i = \lambda_1 a_1 (\frac{f_1}{a_1} - \frac{f_2}{a_2}) + (\lambda_1 a_1 + \lambda_2 a_2)(\frac{f_2}{a_2} - \frac{f_3}{a_3}) + \ldots + (\lambda_1 a_1 + \ldots$$
$$\ldots + \lambda_{s-1} a_{s-1})(\frac{f_{s-1}}{a_{s-1}} - \frac{f_s}{a_s}) + (\lambda_1 a_1 + \ldots + \lambda_s a_s)\frac{f_s}{a_s}.$$

Но $\lambda_1 a_1 + \ldots + \lambda_s a_s = 0$, т.к. $St(\sum \lambda_i f_i) < X^\alpha$. $\square$

Доказательство теоремы. Импликация в правую сторону очевидна.
$\Longleftarrow$ Покажем, что если $f \in I$, то $f = \sum h_i g_i$ и $St(f)$ равен старшему из $St(h_i)St(g_i)$. Пусть X^δ — старший из мономов $St(h_i)St(g_i)$ и $h_i = b_i X^{\beta_i} + \ldots$, $g_i = c_i X^{\gamma_i} + \ldots$. Если он не равен $St(f)$, то он больше чем $St(f)$. Будем считать, что $St(h_i)St(g_i) = X^\delta$ при $i = 1..M$ и $X^\delta > St(h_i)St(g_i)$ при $i = M+1..t$.

Заметим, что многочлен $g = \sum_{i=1}^{M} b_i X^{\beta_i} g_i$. Его старший моном такой же, как и у f, а значит коэффициенты при X^δ сократятся. Поэтому многочлен g

удовлетворяет условиям леммы, и, следовательно,

$$g = \sum_{1 \leqslant i \leqslant j \leqslant M} \mu_{ij} S(b_i X^{\beta_i} g_i, b_j X^{\beta_j} g_j). \tag{12}$$

Нетрудно проверить,

$$S(b_i X^{\beta_i} g_i, b_j X^{\beta_j} g_j) = \frac{X^\delta}{c_i X^{\gamma_i}} g_i - \frac{X^\delta}{c_j X^{\gamma_j}} g_j = \frac{X^\delta}{X^{\gamma_{ij}}} S(g_i, g_j),$$

где $X^{\gamma_{ij}}$ — наименьшее общее кратное X^{γ_i} и X^{γ_j}. По условию $S(g_i, g_j)$ редуцируется к нулю, а значит и $S(b_i X^{\beta_i} g_i, b_j X^{\beta_j} g_j)$ тоже, т.е.

$$S(b_i X^{\beta_i} g_i, b_j X^{\beta_j} g_j) = \sum h_l^{(ij)} g_l,$$

где наибольшее из $St(h_l^{(ij)}) St(g_l)$ совпадает со $St(S(b_i X^{\beta_i} g_i, b_j X^{\beta_j} g_j))$.

Но $St(b_i X^{\beta_i} g_i) = St(b_j X^{\beta_j} g_j) = X^\delta$, а значит у $St(S(b_i X^{\beta_i} g_i, b_j X^{\beta_j} g_j))$ старший член уже меньше, чем X^δ. Из (12) получим

$$g = \sum_{1 \leqslant i \leqslant j \leqslant M} \mu_{ij} \sum h_l^{(ij)} g_l.$$

Но тогда разложение $f = g + \ldots$ противоречит предположению о минимальности X^δ, а значит $X^\delta = St(f)$.□

Алгоритм Бухбергера Теорема показывает, что базис Грёбнера можно построить с помощью следующего алгоритма.

Пусть $I = \langle f_1, \ldots, f_s \rangle$.

1. Проверим все ли $S(f_i, f_j)$ редуцируются к нулю по модулю $f_1, \ldots, f_s$. Если это так, то $f_1, \ldots, f_s$ базис Грёбнера, если нет, то
2. Добавим к набору многочленов редукцию $S(f_i, f_j)$.

Приведенный базис Грёбнера

Определение 48 *Базис Грёбнера $g_1, \ldots, g_t$ минимальный, если $g_i = X^{\alpha_i} + \ldots$ и X^{α_i} и X^{α_j} не делятся друг на друга при $i \neq j$.*

Remark 17 *У любого идеала есть минимальный базис Грёбнера.*

Теорема 35 *Пусть $g_1, \ldots, g_t$ и $f_1, \ldots, f_s$ минимальные базисы Грёбнера идеала I. Тогда $s = t$ и $St(g_i) = St(f_{\sigma(i)}), \sigma \in S_t$.*

Определение 49 *Базис Грёбнера $g_1, \ldots, g_t$ приведенный, если $g_i = X^{\alpha_i} + \ldots$ и g_i равен остатку g_i при делении на $g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_t$ (т.е. ни один из мономов, входящих в g_i не делится на X^{α_j} при $i \neq j$).*

Remark 18 *Приведенный базис Грёбнера является минимальным.*

Теорема 36 *У любого идеала существует единственный приведенный базис Грёбнера.*

Доказательство. Пусть $g_1, \ldots, g_t$ минимальный базис Грёбнера идеала I. Рассмотрим h_1 равный остатку g_1 при делении на $g_2, \ldots, g_t$, h_i равный остатку g_i при делении на $h_1, \ldots, h_{i-1}, g_{i+1}, \ldots, g_t$ $i = 2..t$. Заметим, что $St(h_i) = St(g_i)$. Теперь нетрудно получить, что $h_1, \ldots, h_t$ приведенный базис Грёбнера идеала I.

Покажем, что приведенный базис Грёбнера единственный. Пусть $g_1, \ldots, g_t$ и $f_1, \ldots, f_s$ приведенные базисы Грёбнера идеала I. Так как они являются минимальными $s = t$ и можно считать, что $St(f_i) = St(g_i)$. Пусть $f_i - g_i \neq 0$, тогда, т.к. $f_i - g_i \in I$ старший член $f_i - g_i$ делится на старший член некоторого g_j, причем $i \neq j$ (т.к. у $f_i - g_j$ степень старшего члена меньше чем у g_i). Но тогда старший член g_j делит какой-то моном из f_i или g_i, что противоречит приведенности. $\square$

2.7 Многочлены от многих переменных: выражение симметрических многочленов через элементарные симметрические.

Многочлены от многих переменных: выражение симметрических многочленов через элементарные симметрические. Формальные производные многочленов и число корней, конечные разности. Интерполяционные многочлены. Многочлены от многих переменных

Определение 50 *Многочлен $f(x_1, \ldots, x_n)$ называется <u>симметрическим</u>, если для любой подстановки $\sigma \in S_n$ выполняется равенство*

$$f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = f(x_1, \ldots, x_n).$$

Основным примером симметрических многочленов служат <u>элементарные</u> симметрические многочлены $\sigma_k(x_1, \ldots, x_n) = \sum_{i_1 < \ldots < i_k} x_{i_1} \cdots x_{i_k}$, где $1 \leqslant k \leqslant n$; Положим $\sigma_0 = 1$, $\sigma_k(x_1, \ldots, x_n) = 0$ при $k > n$.

Элементарные симметрические многочлены можно задавать с помощью производящей функции

$$\sigma(t) = \sum_{k=0}^{\infty} \sigma_k t^k = \Pi_{i=1}^{\infty}(1 + tx_i).$$

Если $x_1, \ldots, x_n$ — корни многочлена $x^n + a_{n-1}x^{n-1} + \ldots + a_0$, то $\sigma_k(x_1, \ldots, x_n) = (-1)^k a_{n-k}$.

Теорема 37 *Пусть* $f(x_1, \ldots, x_n)$ — *симметрический многочлен. Тогда существует единственный многочлен* $g(y_1, \ldots, y_n)$, *что* $f(x_1, \ldots, x_n) = g(\sigma_1, \ldots, \sigma_n)$.

3 Обозначения

- Для множества X $|X|$ обозначает мощность множества X.
- $\mathrm{End}(V)$ кольцо эндоморфизмов векторного пространства V.
- $\mathrm{GL}(V) = \mathrm{Aut}(V) = (\mathrm{End}(V))^*$.

Список литературы

[1] http://alexei.stepanov.spb.ru/students/temp/conspect.pdf

[2] Кострикин А.И. "Введение в алгебру". Основы алгебры: Учебник для вузов. — М.: Физматлит. 1994.— 320 с. — ISBN 5-02-014644-7.

[3] Кострикин А.И. "Введение в алгебру". Часть III. Основные структуры: Учебник для вузов.— 3-е изд. — М.: ФИЗМАТЛИТ, 2004.— 272 с. — ISBN 5-9221-0489-6.

[4] Алексеев В.Б. "теорема Абеля в задачах и решениях— М.: МЦНМО, 2001.

[5] А.Л.Городенцев. Алгебра. Учебник для студентов-математиков. Часть I. "МЦ НМО 2013

[6] http://alexei.stepanov.spb.ru/students/algebra3/Berns

[7] Н.А. Вавилов "Конкретная теория групп"

[8] К. Айерленд М.Роузен "Классическое введение в современную теорию чисел"

[9] Н. Коблиц "Курс теории чисел и криптографии"Москва: Научное изд-во ТВП, 2001, x+254 с.

[10] http://www.mathblog.dk/course-linear-algebra-gilbert-strang/

[11] http://mit.spbau.ru/sewiki/index.php/%D0%90%D0

[12] http://mit.spbau.ru/sewiki/images/3/3e/02_linear_algebra.pdf

[13] http://mit.spbau.ru/sewiki/index.php/

[14] Прасолов В.В. "Многочлены"