Московский физико-технический институт
Физтех-школа прикладной математики и информатики

АЛГЕБРА И ГЕОМЕТРИЯ

II СЕМЕСТР

Лектор: *Вадим Владимирович Штепин*

h\nu

Автор: *Киселев Николай*
Репозиторий на Github

весна 2025

Содержание

1 Алгебра многочленов

Определение 1.1. Многочленом называется функция $f : \mathbb{R} \to \mathbb{R}, f = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$

Определение 1.2. $\mathbb{F}[x]$ — множество всех многочленов над $\mathbb{F}$ (с коэффициентами в $\mathbb{F}$)

1.1 Операции над многочленами

1. $+$ — сложение
2. $\cdot$ — умножение
3. $\cdot\lambda$ — домножение на константу

Замечание. Многочлены над $\mathbb{R}$ образуют коммутативное кольцо

Определение 1.3. Алгебра над полем $\mathbb{F}$ называется называется множество A, с определенными на нем операциями $+, \cdot, \cdot\lambda$, которое удовлетворяет следующим условиям:

1. $(A, +, \cdot\lambda)$ — линейное пространство над $\mathbb{F}$
2. $(A, +, \cdot)$ — кольцо (необязательно коммутативное)
3. $\lambda(xy) = x(\lambda y) = (\lambda x)y, \lambda \in \mathbb{F}, x, y \in A$

Пример.

1. $\mathbb{R}[x]$
2. $M_n(\mathbb{F})$
3. $\mathbb{Z}_p[x]$

Замечание. Возникает проблема: в $\mathbb{Z}_p[x]$ сущесвтует многочлен $x^p - x \equiv 0 \forall x \in \mathbb{Z}_p$. Но тогда у нас будет конечный базис в $\mathbb{Z}_p[x]$, чего не хотелось бы. Определим многочлен по-другому:

Определение 1.4. Многочленом над коммутативным кольцом с 1 R называется бесконечная пооследовательность $a_0, a_1 \dots$, в которой лишь конечное число коэффициентов отличны от 0. Такие пооследовательности называются финитными.

1.2 Операции над новыми многочленами

Пусть $A = (a_i), B = (b_i)$

1. $A + B = C \Leftrightarrow c_i = a_i + b_i$
2. $A \cdot B = C \Leftrightarrow c_k = \sum_{i=0}^{k} a_i b_{k-i}$
3. $A \cdot \lambda = C \Leftrightarrow c_k = \lambda \cdot a_i$

Утверждение 1.1. *$R[x]$ — коммутативное кольцо относительно "+", "·"*

Доказательство.

1. $(R[x], +)$ — абелева группа (очев)
2. $A \cdot B = B \cdot A$ — тут мы пользуемся тем, что R — коммутативное кольцо. Поэтому в сумме $\sum_{i=0}^{k} a_i b_{k-i}$ если переставить множители местами, ничего не поменяется
3. $A(BC) = (AB)C$

$$\sum_{i=0}^{n} a_i \left(\sum_{j=0}^{n-i} b_j c_{n-i-j} \right) = \sum_{i=0}^{k} \sum_{j=0}^{n-i} a_i b_j c_{n-i-j} = \sum_{i+j+k=n} a_i b_j c_k = \sum_{k=0}^{n} c_k \left(\sum_{i=0}^{n-k} a_i b_{n-k-i} \right)$$

4. $A(B + C) = AB + AC$ — Достаточно раскрыть скобки, чтобы проверить, мне лень техать.

$\square$

Следствие. $R[x]$ — бесконечномерное линейное пространство с базисом $1, x, x^2 \dots$.

Следствие. Нетрудно проверить, что в $R[x]$, $1 = (1, 0, 0, \dots)$. Аналогично, $x^n = (\underbrace{0, 0, \dots 0}_{n}, 1, 0, 0, \dots)$

Определение 1.5. Старший коэффициент — последний ненулевой элемент последовательности.

Определение 1.6. Индекс старшего коэффициента называется степенью многочлена $\deg P$. У многочлена $(0, 0, \dots)$ степень зависит от контекста. Мы будем считать, что его степень $-\infty$.

Определение 1.7. Кольцо с $1 \neq 0$ называется областью целостности, если в нем нет делителей нуля.

Утверждение 1.2. *Пусть R — область целостности. Тогда $ab = ac, a \neq 0 \Rightarrow b = c$*

Доказательство.

$$a(b - c) = 0$$

$$b - c = 0$$

$$b = c$$

$\square$

Утверждение 1.3. *$A, B \in R[x], 1 \in R$. Тогда:*

1. $\deg A + \deg B \leqslant \max(\deg A, \deg B)$
2. $\deg AB \leqslant \deg A + \deg B$

Причем, если R — область целотности, то во втором пункте будет равенство.

Доказательство. Все понятно $\square$

Следствие. Если R — область целостности, то $R[x]$ — тоже.

Определение 1.8. Многочлен от n переменных определяется рекурсивно: многочлен от одной переменной — как мы определяли выше, далее $R[x_1, x_2, \dots x_n] = R[x_1, x_2, \dots x_{n-1}][x_n]$.

1.3 Деление многочленов с остатком

Теорема 1.1. *Пусть* F *— поле,* $A, B \in F[x], B \neq 0$. *тогда*

1. $\exists! Q, R : A = BQ + R, \deg R < \deg B$

Доказательство. Существование доказывается алгоритмом деления в столбик. Проверим единственность:

$$BQ + R = BS + T$$

$$BQ - BS = T - R$$

$$\deg(B(Q - S)) > \deg(T - R)$$

Противоречие □

Теорема 1.2 (Безу)**.** *Пусть* $P \in F[x]$. *Тогда* $P(x) - P(c) \vdots (x - c)$

Доказательство. Разделим многочлен P на $x - c$ с остатком. Получится $P = Q(x - c) + R$, причем R — константа. Тогда подставим $x = c$, получим, что $R = P(c)$. □

1.3.1 Схема Горнера

Задан многочлен:

$$P(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n, \quad a_i \in \mathbb{R}$$

Пусть требуется вычислить значение данного многочлена при фиксированном значении $x = x_0$. Представим многочлен $P(x)$ в следующем виде:

$$P(x) = a_0 + x(a_1 + x(a_2 + \cdots x(a_{n-1} + a_nx) \ldots))$$

Определим следующую последовательность:

$$b_n = a_n,$$

$$b_{n-1} = a_{n-1} + b_nx_0,$$

$$\vdots$$

$$b_i = a_i + b_{i+1}x_0,$$

$$\vdots$$

$$b_0 = a_0 + b_1x_0.$$

Искомое значение $P(x_0)$ есть b_0. Покажем, что это так.

В полученную форму записи $P(x)$ подставим $x = x_0$ и будем вычислять значение выражения, начиная с внутренних скобок. Для этого будем заменять подвыражения через b_i

$$\begin{aligned} P(x_0) \quad &= a_0 + x_0(a_1 + x_0(a_2 + \cdots x_0(a_{n-1} + a_nx_0) \ldots)) = \\ &= a_0 + x_0(a_1 + x_0(a_2 + \cdots x_0b_{n-1} \ldots)) = \\ &\ \vdots \\ &= a_0 + x_0b_1 = \\ &= b_0. \end{aligned}$$

1.4 НОД двух многочленов. Алгоритм Евклида

Определение 1.9. Многочлен f делится на g, если $f = gh$ для некототорого h

Определение 1.10. Многочлены f, g называются ассоциированными, если $f \vdots g, g \vdots f$.

Определение 1.11. Многочлен d называется Наибольшим общим делителем двух многочленов f, g, если:

1. $f \vdots d, g \vdots d$

2. $f \vdots d', g \vdots d' \Rightarrow d \vdots d', d \vdots d'$

Теорема 1.3 (О представлении НОДа)**.**

1. *НОД любых двух многочленов существует*

2. *НОД любых двух многочленов представим в виде их линейной комбинации*

2 Неприводимые многочлены

Определение 2.1. Пусть F — поле, $F[x]$ — кольцо многочленов над F. Многочлен $P \in F[x], \deg P > 0$ называется наприводимым, если $AB = P \Rightarrow \deg A = 0 \vee \deg B = 0$. Иначе говоря, многочлен неприводим над полем F, если он не раскладывается в произведение многолченов более низких степеней.

Пример. $x^2 + 1 \in \mathbb{R}[x]$ — неприводим. Очев, т.к. не имеет корней.

Пример. $x^2 + 1 = (x - i)(x + i) \in \mathbb{C}[x]$

Утверждение 2.1. *P — неприводимый, тогда* $\forall A : (A, P) = \left[\begin{array}{l} \sim 1 \\ \sim P \end{array}\right.$

Доказательство. По-другому быть не может, т.к. у P нет делителей, кроме 1 и самого себя. □

Лемма 2.1 (Евклида)**.** *Пусть P — неприводиный многочлен, $AB \vdots P \Rightarrow A \vdots P \vee B \vdots P$.*

Доказательство. От противного, тогда $A \not\vdots P, B \not\vdots P$. Тогда по теореме о представлении НОДа в виде линейной комбинации:

$$(A, P) = u_1 A + u_2 P = 1$$

$$u_1 AB + u_2 PB = B \vdots P$$

Противоречие □

Теорема 2.1 (Основная Теорема Арифметики)**.** *Пусть A — ненулевой многочлен из $F[x], F$ — поле. Тогда $\exists! P_1, P_2 \dots P_n$ с точностью до перестановки множителей и домножения на константу, где P_i — неприводим и $A = \Pi_{i=1}^{n} P_i$.*

Доказательство.

Существование. По индукции: либо он неприводим и очев, либо нет, тогда разложим и для каждого множителя разложим его.

Единственность. Пусть не единственно, будем тогда сокращать на $P_1, P_2, \ldots$. Получим, что в разложении должны содержаться многочлены, пропорциональные $P_1, \ldots P_n$ соответственно

□

Следствие. Если $A \vdots P$, то разложение A является подмножеством разложения P

2.1 Корни многочленов

Определение 2.2. Многолчен P имеет корень c кратности k, если $P \vdots (x-c)^k, P \not\vdots (x-c)^{k+1}$

Определение 2.3. Если многочлен раскладывается в произведение линейных множителей над полем F, то он называется линейно факторизуемым над ним.

Замечание. Основная Теорема Арифметики неверна (разложение может быть не единственным) для случаев, когда F — коммутативное кольцо.

2.2 Основная Теорема Алгебры

На лекции было миллион лемм и вспомогательных утвеждений, но я просто вставлю доказательство из лекции по матану, потому что я так могу (и потому что доказательство идейно не отличается от него).

Теорема 2.2 (Больцано-вейерштрасса)**.** *Пусть $\{z_n\}$ ограничена, то есть $\exists C > 0 : \forall n(|z_n| \leqslant C)$. Тогда у нее существует сходящаяся подпоследовательность*

Доказательство. По обычной теореме Больцано-Вейерштрасса, ищем подпоследовательность, действительная часть которой имеет предел. В ней выбираем последовательность, мнимая часть которой имеет предел. Получили. □

Определение 2.4. Функция $f : E \subset \mathbb{C} \to \mathbb{C}$ непрерывна в точке z_0, если $\forall \{z_n\} \subset E(z_n \to z_0 \Rightarrow f(z_n) \to f(z_0))$.

Утверждение 2.2. *Пусть $f : \{|z| \leqslant R\} \to \mathbb{R}$ непрерывна на $\mathbb{C}$. Тогда $\exists z_0, |z_0| \leqslant R, \inf_{|z| \leqslant R} f(z) = f(z_0)$.*

Доказательство.

$$m = \inf_{|z| \leqslant R} f(z)$$

Рассмотрим $r_n \to m, r_n > m$. $\exists z_n, |z_n| \leqslant R, m \leqslant f(z_n) \leqslant r_n$ В частности, $f(z_n) \to m$. При этом, $\{z_n\}$ — ограничена, $\Rightarrow \exists z_{n_k} \to z_0 \Rightarrow |z_0| \leqslant R$. В частности $||z| - |z_0|| \leqslant |z - z_0|$. В силу непрерывности f в z_0: $f(z_{n_k}) \to f(z_0), f(z_{n_k}) \to m \Rightarrow m = f(z_0)$. □

Теорема 2.3. *Пусть $f \in \mathbb{C}[z], \deg f > 0$. Тогда f имеет корень.*

Доказательство. 1. Покажем, что $\exists z_0 \in \mathbb{C} \inf_{z\in\mathbb{C}} |P(z)| = |P(z_0)|$. Для начала возьмем $R \geqslant 1$.

$$\left|\sum_{k=0}^{n-1} a_k z^k\right| \leqslant \sum_{k=0}^{n-1} |a_k||z|^k \leqslant |z|^n \sum_{k=0}^{n-1} |a_k| = A$$

Теперь рассмотрим $|z| \geqslant \frac{2A}{|a_n|} \Rightarrow A|z|^{n-1} \leqslant \frac{1}{2}|a_n||z|^n$. Тогда $|P(z)| \geqslant |a_n z^n| - \left|\sum_{k=0}^{n-1} a_k z^k\right| = \frac{1}{2}|a_n|z^n$. Возьем радиус $R = \max\left\{1, \frac{2A}{|a_n|}, \sqrt[n]{\frac{2|a_0|}{|a_n|}}\right\}$. Тогда при $|z| \geqslant R$ выполнено $|P(z)| \geqslant |P(0)|$, поэтому $\inf_{\mathbb{C}} |P(z)| = \inf_{|z|\leqslant R} |P(z)|$. Но тогда найдется такое $|z_0| \leqslant R$, что у нас $\inf_{\mathbb{C}} |P(z)| = |P(z_0)|$

2. Докажем, что если $P(z_0) \neq 0$, то $\exists z_* \in \mathbb{C} |P(z_*)| < |P(z_0)|$. Рассмотрим многочлен $Q(z) = \frac{P(z+z_0)}{P(z_0)}$. Тогда $Q(0) = 1$. Обозначим через α_k — наименьший коэффициент Q, отличный от 0 и $k \geqslant 1$. $Q(z) = 1 + \alpha_k z^k + \ldots$. Возьмем $z_1 \in \mathbb{C}$, $\alpha_k z_1^k = -1$, пусть $t \in (0, 1)$. $Q(tz_1) = 1 - t^k + t^{k+1}\varphi(t)$, $\varphi(t)$ — многочлен степени $n-k-1$. C — наибольший из модулей коэффициентов $\varphi(t)$, тогда $|\varphi(t)| \leqslant C(n-k)$. Тогда

$$Q(tz_1) < 1 - t^k|\varphi(t)| \leqslant 1 - t^k(1 - tC(n-k))$$

Рассмотрим произвольное $t \in \left(0, \frac{1}{C(n-k)}\right)$. Тогда $|Q(tz_1)| < 1$. Но тогда при $z_* = tz_1$ верно, что $|P(z_*)| < |P(z_0)|$

Но тогда, точка z_0 (из первого пункта) такова, что $P(z_0) = 0$.

□

2.3 Следствия из основной теоремы алгебры

Определение 2.5. Поле F называется алгебраически замкнутым, если $\forall f \in F[x], \deg f > 0$ он имеет хотя бы один корень.

Следствие. Поле $\mathbb{C}$ — алгебраически замкнуто

Следствие. Любой многолчен из $\mathbb{C}$ — линейно факторизуем.

Следствие. Любой многолчен из $\mathbb{R}$ раскладывается в произведение многочленов 1 и 2 степени

Доказательство. Пусть $c \notin \mathbb{R}$ — корень f. Тогда $\overline{c}$ — тоже. Но тогда $f \vdots (x-c)(x-\overline{c})$ □

2.4 Формальная производная

Определение 2.6.

$$(a_n x^n + \cdots + a_1 x + a_0)' = n a_n x^{n-1} + \cdots + 2a_2 x + a_1$$

Замечание. Все свойства обычной производной верны

1. $(\alpha P + \beta Q)' = \alpha P' + \beta Q'$
2. $(PQ)' = P'Q + PQ'$

3. $(P_1P_2P_3\dots P_{n-1}P_n)' = P_1'P_2P_3\dots P_{n-1}P_n + P_1P_2'P_3\dots P_{n-1}P_n + \dots P_1P_2P_3\dots P_{n-1}P_n'$
4. $(P^n)' = nP^{n-1}P'$

Доказательство. 1. Доказательство по определению:
$\left(\sum_{i=1}^{k}\alpha_i x^i\right)' + \left(\sum_{i=1}^{i}\beta_k x^{i-1}\right)' = \left(\sum_{i=1}^{k} i\alpha_i x^{i-1}\right) + \left(\sum_{i=1}^{i} i\beta_i x^{i-1}\right)' =$
$= \sum_{i=0}^{k}(\alpha_i+\beta_i)\cdot ix^{i-1} = \left(\sum_{i=0}^{k}(\alpha_i+\beta_i)x^i\right)'$

2. Раскроем скобки: $\left(\sum_{i=0}^{k}\alpha_i x^i\cdot Q(x)\right)' = \left(\sum_{i=0}^{k}\sum_{j=0}^{l}\alpha_i\beta_j x^{i+j}\right)' =$
$= \sum_{i=0}^{k}\sum_{j=0}^{l}(i+j)\alpha_i\beta_j x^{i+j-1} = \sum_{i=0}^{k}\sum_{j=0}^{l} i\alpha_i\beta_j x^{i+j-1} + \sum_{i=0}^{k}\sum_{j=0}^{l} j\alpha_i\beta_j x^{i+j-1} =$
$= P'Q + PQ'$

3. Индукция: *База* $n=2 \to$ см п. 2. *Переход:* Объединим $P_{n-1}P_n$ в $Q \to 2$ раза п. 2.

4. Применяем п. 4 для $P_1 = P_2 = \dots = P_{n-1} = P_n = P$

□

3 Рациональные дроби

3.1 Поле частных

Пусть A — область целостности, обозначим $A^* = A\setminus\{0\}$. Рассмотрим множество $A\times A^* = \{(f,g)\} = \{\frac{f}{g}\}$ и введем на нем следующие операции и отношения:

3.2 Отношение равенства

$$\frac{f_1}{g_1} = \frac{f_2}{g_2} \Leftrightarrow f_1g_2 - f_2g_1 = 0$$

3.3 Операция сложения

$$\frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{f_1g_2+f_2g_1}{g_1g_2}$$

Доказательство корректности.

$$\frac{f_1}{g_1} = \frac{a}{b}, \frac{f_2}{g_2} = \frac{c}{d}, \frac{f_1g_2+f_2g_1}{g_1g_2} =^? \frac{ad+bc}{bd}$$

$$(f_1g_2+f_2g_1)bd =^? (ad+bc)g_1g_2$$

$$f_1g_2bd + f_2g_1bd =^? adg_1g_2 + bcg_1g_2$$

$$f_1g_2bd + f_2g_1bd - adg_1g_2 - bcg_1g_2 =^? 0$$

$$dg_2\underbrace{(bf_1 - g_1a)}_{0} - bg_1\underbrace{(f_2d - cg_2)}_{0} = 0$$

□

Замечание. $\frac{0}{f}, f \neq 0$ — нейтральный по сложению

3.4 Операция умножения

$$\frac{f_1}{g_1}\frac{f_2}{g_2} = \frac{f_1 f_2}{g_1 g_2}$$

Доказательство корректности.

$$\frac{f_1}{g_1} = \frac{a}{b}, \frac{f_2}{g_2} = \frac{c}{d} \Rightarrow \frac{f_1 f_2}{g_1 g_2} = \frac{ac}{bd}$$

Доказательство предоставляется читателю в качестве нетрудного упражнения □

Определение 3.1. Полученное поле называется полем частных области целостности A и обозначается $Q(A)$

Определение 3.2. Полученное поле называется полем частных области целостности A и обозначается $Q(A)$

Пример. $Q(\mathbb{Z}) = \mathbb{Q}$

Пример. $Q(F) = F$

3.5 Поле рациональных дробей

Определение 3.3. $Q(F[x]) = F(x)$ — поле рациональных дробей

Определение 3.4. $\deg \frac{f}{g} = \deg f - \deg g$. Если $deg \frac{f}{g} < 0$, то дровь называется правильной, иначе — неправильной

Утверждение 3.1. *Любая рациональная дробь представима единственным образом в виде $p + \frac{q}{r}$, где p — многочлен, а $\frac{q}{r}$ — рациональная дробь*

Доказательство. Делим с остатком и очев. □

Утверждение 3.2.

$$\deg\left(\frac{f_1}{g_1} + \frac{f_2}{g_2}\right) = \max\left(\deg \frac{f_1}{g_1}, \deg \frac{f_2}{g_2}\right)$$

$$\deg\left(\frac{f_1}{g_1} \cdot \frac{f_2}{g_2}\right) = deg \frac{f_1}{g_1} + \deg \frac{f_2}{g_2}$$

Теорема 3.1. *Путсь $\frac{f}{g}$ — правильная рациональная дробь, $g = g_1 g_2 \dots g_n$, причем $(g_i, g_j) = 1$. Тогда существует единственный набор $f_1, f_2 \dots f_n$, таких, что:*

$$\frac{f}{g} = \frac{f_1}{g_1} + \frac{f_2}{g_2} + \dots + \frac{f_n}{g_n}, \deg f_i < \deg g_i$$

Доказательство.

Существование. ведем индукцию по n

База: $n = 1$. Очевидно.

Переход: Обозначим $h = g_1 g_2 \dots g_{n-1}$. Тогда

$$\frac{f}{g} = \frac{\mu f}{g_1} + \frac{\lambda f}{h}$$

Где $\lambda g + \mu h = 1 = (g, h)$ (существуют из разложения НОДа). Но тогда по предположению индукции, разложим $\frac{\lambda f}{h}$ и получим желаемое

Единственность. ведем индукцию по n

База: $n = 1$. Очевидно.

Переход: Обозначим $h = g_1 g_2 \dots g_{n-1}$. Пусть это не так. Но тогда у нас есть два разложения, приведем в каждом из них дроби с $g_i, i \neq n$ к общему знаменателю. Тогда сущесвтуют a, b, c, d, такие, что

$$\frac{f}{g} = \frac{a}{g_n} + \frac{b}{h} = \frac{c}{g_n} + \frac{d}{h}$$

$$ah + bg_n = ch + dg_n$$

Но тогда $h(a - c) = g_n(b - d)$. Т.к. $\deg(b - d) < h \Rightarrow (g_n, h) \neq 1$, противоречие

□

Замечание. Если в предыдущем утверждении $g_1, g_2, \dots g_n$ — неприводимые множители, то они взаимно просты между собой, но тогда любая правильная рациональная дробь единственным образом представляется в таком виде.

Определение 3.5. Правильная рациональная дробь $\frac{f}{g}$ называется простейшей, если ее знаменатель — степень неприводимого многочлена.

Следствие. Любая правильная рациональная дробь единственным образом представима в виде суммы простейших дробей.

Теорема 3.2. *Пусть f — ненулевой многочлен, p — многочлен положительной степени. Тогда $\exists!$ представление f в виде:*

$$f = \varphi_0 + \varphi_1 p + \varphi_2 p^2 + \dots + \varphi_n p^n, \deg \varphi_i < \deg p$$

Доказательство.

Существование. ведем индукцию по степени f.

База: $\deg f = 1$. Очевидно.

Переход: Разделим f на p с остатком, получится $\varphi_0 + rp = f$. Получили φ_0, по предположению индукции разложим r и получим разложение

Единственность. Пусть есть два разложения. Вычтем одно из другого: с одной стороны получим 0, с другой стороны, рассмотрим минимальный индекс, где $\varphi_i \neq \varphi_i'$ и получим ненулевой многочлен. Противоречие.

□

4 Инвариантные пространства

Теперь снова вернемся к линейным операторам

4.1 Напоминание

Определение 4.1. $\varphi : V \to V$ называется линейным оператором, если он удовлетворяет следующим условиям:

1. Аддитивность — $\varphi(x + y) = \varphi(x) + \varphi(y)$
2. Однородность — $\varphi(\lambda x) = \lambda\varphi(x)$

Эти два условия можно заменить одним — линейностью

Пусть $\mathfrak{E}$ — базис в V. Т.к. линейный оператор линеен, то нам достаточно знать его значения на элементах $\mathfrak{E}$ (все остальное узнаем из линейности). Пусть $\varphi(e_i) = \sum_{k=1}^{n} a_{ki}e_k$. Тогда:

$$\varphi(\mathfrak{E}) = \mathfrak{E} \cdot A$$

Где $[A]_{ij} = a_{ij}$.

Определение 4.2. $\mathfrak{L}(V)$ — пространство всех линейных отображений

Причем линейные операторы можно умножать:

$$\varphi \cdot \psi(x) = \varphi(\psi(x))$$

И тогда выполнено:

$$\varphi \longleftrightarrow_{\mathfrak{E}} A, \psi \longleftrightarrow_{\mathfrak{E}} B \Rightarrow \varphi\psi \longleftrightarrow \mathfrak{E}AB$$

4.2 Инвариантное подпространство

Определение 4.3. Подпространство $U \leqslant V$ называется инвариантным относительно оператора φ, если $\forall x \in U \ \ \varphi(x) \in U$. Иначе говоря, $\varphi(U) \subset U \Leftrightarrow \varphi(U) \leqslant U$.

Определение 4.4. Базис $\mathfrak{E}$ в V называется согласованным с инвариантным подпространством U, если $e_1, e_2, \ldots e_k$ — базис в U.

Утверждение 4.1. *Подпространство U инвариантно относительно $\varphi \Leftrightarrow$ в базисе $\mathfrak{E}$, согласованным с U, выполнено:*

$$A_\varphi = \left(\begin{array}{c|c} A_U & B \\ \hline 0 & C \end{array}\right), A_U \in M_{k\times k}, k = \dim U$$

Доказательство. Пусть $\mathfrak{E}$ — согласован с U. U — инвариантен относительно $\varphi \Leftrightarrow \varphi(e_j) \in U = \langle e_1, e_2, \ldots e_k\rangle, i \leqslant j \leqslant k$

$$\Leftrightarrow \varphi(e_j) = \begin{pmatrix} *_1 \\ \vdots \\ *_k \\ 0 \\ \vdots \\ 0 \end{pmatrix} \Rightarrow A_\varphi = \left(\begin{array}{c|c} A_U & B \\ \hline 0 & C \end{array}\right), A_U \in M_{k\times k}, k = \dim U$$

□

Утверждение 4.2. *Если U, V — инвариантны относительно $\varphi : V \to V$, то $U \cap V, U + V$ — тоже.*

Доказательство.

$$\varphi(U \cap W) \leqslant \underbrace{\varphi(U)}_{\leqslant U} \cap \underbrace{\varphi(W)}_{\leqslant W} \leqslant U \cap W$$

$$\varphi(U + W) = \varphi(U) + \varphi(W) \leqslant U + W$$

□

Утверждение 4.3 (О коммутатирующих операторах)**.** *Пусть $\varphi, \psi \in \mathfrak{L}(V), \varphi \cdot \psi = \psi \cdot \varphi$. Тогда подпространства $\ker \varphi, \ker \psi, Im\varphi, Im\psi$ инвариантны относительно каждого из этих операторов.*

Доказательство.

1. $\varphi(\ker \varphi) = \{0\}$
2. $\varphi(Im\varphi) \leqslant Im\varphi$ — очев
3. $\varphi(\ker \psi) \leqslant \ker \psi$
$$\psi(\varphi(\ker \psi)) = \varphi(\psi(\ker \psi)) = \{0\} \Rightarrow \varphi(\ker \psi) \leqslant \ker \psi$$
4. $\varphi(Im\psi) \leqslant Im\psi$
$$\varphi(x) = \varphi(\psi(x')) = \psi(\varphi(x')) \leqslant Im\varphi$$

□

Короче тут лектор так разогнался, что я ничего не успел записать, поэтому вот вам основные определения:

Определение 4.5. Ненулевой вектор x называется собственным, если $\varphi(x) = \lambda x$

Определение 4.6. Собственным подпространством линейного преобразования φ называется пространство $\ker(\varphi - \lambda \cdot \mathrm{id})$

4.3 Структура линейного оператора

Определение 4.7. $\chi_A(\lambda) = \det(A - \lambda E)$ — характеристический многочлен линейного оператора A.

Утверждение 4.4 (О свойствах характеристического многочлена)**.**

1. *$\chi_A(\lambda) = 0, \lambda \in F$, тогда λ — собственное значение оператора A.*
2. *$\chi_A(\lambda)$ не зависит от выбора базиса, в котором записывается A.*

Доказательство.

1. $Ax = \lambda x \Leftrightarrow (A - \lambda E)x = 0$ имеет нетривиальное решение $\Leftrightarrow \det(A - \lambda E) = 0$
2. $\det(SAS^{-1} - \lambda E) = \det(SAS^{-1} - \lambda SES^{-1}) = \det S \det S^{-1} \det(A - \lambda E) = \det(A - \lambda E)$

□

Определение 4.8. Линейный оператор называется диагонализируемым, если существует базис, в котором его матрица является диагональной

Теорема 4.1 (Критерий диагонализируемости). *Пусть $\varphi : V \to V$ — линейный оператор, $\lambda_1, \lambda_2 \dots \lambda_k$ — все попарно различные корни характеристического многочлена. Тогда следующие утверждения эквивалентны:*

1. *φ — диагонализируема*
2. *В V суещствует бащис, состоящий из собственных векторов для φ*
3. *$V = V_{\lambda_1} \oplus V_{\lambda_2} \oplus \dots \oplus V_{\lambda_k}$*

Доказательство.

$1 \Rightarrow 2$ Рассмотрим базис, в котором матрица имеет диагоанльный вид $\mathfrak{E}$. Но тогда $\forall e \in \mathfrak{E}$: $Ae = \lambda_i e$ для некоторого i. Но тогда этот базис состоит из собственных векторов.

$2 \Rightarrow 3$ Рассмотрим отдельно базисы, отвечающие собственным значениям $\lambda_1, \lambda_2 \dots \lambda_k$. Они образуют базисы пространств $V_{\lambda_1}, V_{\lambda_2}, \dots V_{\lambda_k}$. Но тогда $V = V_{\lambda_1} \oplus V_{\lambda_2} \oplus \dots \oplus V_{\lambda_k}$

$3 \Rightarrow 1$ Рассмотрим объединение базисов этих пространств. Т.к. каждый вектор полученного базиса будет собственным, в каждой строке и каждом столбце матрицы будет записано ровно одно число. Но тогда можно поменять местами векторы базиса так, чтобы матрица была диагональной

□

4.4 Алгебраическая и Геометрическая кратности

Определение 4.9. Алгебраической кратностью собственного значения λ_0 многочлена $\chi_A(\lambda)$ называется кратность его как корня данного многочлена.

Определение 4.10. Геометрической кратностью собственного значения λ_0 называется $\dim V_{\lambda_0}$

Утверждение 4.5. *Пусть $\varphi : V \to V$ — линейный оператор, $U \leqslant V$, U инвариантно относительно phi, $\psi = \varphi|_U \in \mathcal{L}(U)$. Тогда $\chi_\varphi \vdots \chi_\psi$*

Доказательство.

$$\mathfrak{E} = (\underbrace{\underbrace{e_1, e_2, \dots e_k}_{\text{Базис } U}, e_{k+1}, \dots e_n}_{\text{Базис } V})$$

Но тогда:

$$A_\varphi = \left(\begin{array}{c|c} A_\psi & B \\ \hline 0 & C \end{array}\right) \Rightarrow \chi_\varphi(\lambda) = |A_\varphi - \lambda E| = |A_\psi - \lambda E||C - \lambda E| = \chi_\psi(\lambda)\chi_C(\lambda)$$

□

Следствие. Пусть λ — собственное значение $\varphi : V \to V$. Тогда $geom(\lambda) \leqslant alg(\lambda)$

Доказательство. Рассмотрим $V_\lambda, \psi = \varphi|_{V_\lambda}$. Тогда

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

И тогда $\chi_\psi(t) = (\lambda - t)^k$, где $k = \dim V_\lambda$ По вышедоказанному утверждению, $\chi_\varphi \vdots \chi_\psi \Rightarrow \chi_\varphi(t) \vdots (\lambda - t)^k \Rightarrow alg(\lambda) \geqslant geom(\lambda)$ □

Следствие. Если χ_φ — не линейно факторизуем, то φ — не диагонализируем

Теорема 4.2. *Пусть $\varphi : V \to V$ — линейные оператор. Тогда он диагонализируем тогда и только тогда, когда*

1. *φ — линейно факторизуем над F*
2. *$\forall i \;\; alg(\lambda_i) = geom(\lambda_i)$*

Доказательство.

- $\Rightarrow$ Т.к. $V = V_{\lambda_1} \oplus V_{\lambda_2} \oplus \dots \oplus V_{\lambda_k}$, то $\dim V = \dim V_{\lambda_1} + \dim V_{\lambda_2} + \dots + \dim V_{\lambda_k}$. Но тогда 1 и 2 верны, т.к. $alg(\lambda_i) \geqslant geom(\lambda_i)$, и, при этом $\sum alg(\lambda_i) = \sum geom(\lambda_i)$.
- $\Leftarrow$ В таком случае $\sum alg(\lambda_i) = \sum geom(\lambda_i)$. Но тогда $\dim V = \sum geom(\lambda_i)$. Но тогда $V = V_{\lambda_1} \oplus V_{\lambda_2} \oplus \dots \oplus V_{\lambda_k}$

□

Определение 4.11. Жорданова клетка порядка n, отвечающая собственному значению λ — это матрица:

$$J_n(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 & 0 \\ 0 & \lambda & 1 & \dots & 0 & 0 \\ 0 & 0 & \lambda & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & 0 & \dots & 0 & \lambda \end{pmatrix}$$

Замечание. Линейной факторизуемости χ_φ недостаточно, чтобы утверждать диагонализируемость φ. Например, $J_n(\lambda)$ не диагонализируема, т.к. $J_n(\lambda) - \lambda E$ имеет размерность решений 2, но $\chi_{J_n(\lambda)}(t) = (\lambda - t)^n$.

Утверждение 4.6. *$\varphi : V \to V, \varphi_\lambda = \varphi - \lambda E$. Тогда следующие утверждения эквивалентны:*

1. *Подпространство $U \leqslant V$ инвариантно относительно φ.*
2. *$\exists \lambda \in F : U$ — инвариантно относительно φ_λ.*

3. $\forall \lambda \in F : U$ — инвариантно относительно φ_λ.

Доказательство.

$1 \Rightarrow 2$ очевидно, $\lambda = 0$

$2 \Rightarrow 3$ $(\varphi - \lambda E)x = \mu x \Rightarrow (\varphi - \lambda E - \lambda_1 E)x = (\mu - \lambda_1)x$

$3 \Rightarrow 1$ Тоже очевидно

□

Утверждение 4.7. *Пусть $\varphi : V \to V$ — линейный оператор и $\chi_\varphi(t)$ линейно факторизуем. Тогда у φ найдется $n-1$ мерное подпространство.*

Я СДАЮСЬ он победил

4.5 Аннулирующие многочлены

Определение 4.12. Пусть V — линейное пространство над полем F, $\varphi : V \to V$ — линейный оператор. Многочлен P называется аннулирующим для оператора φ, если $P(\varphi) = 0$

Существование такого многочлена можно обосновать по Теореме Гамильтона-Кэли, а можно и другим способом: Заметим, что размерность пространства линейных операторов $\varphi : V \to V = (\dim V)^2$. Поэтому, операторы $E, \varphi, \varphi^2 \dots \varphi^{n^2}$ линейно зависимы. Но тогда $\exists \lambda_i : E\lambda_0 + \varphi\lambda_1 + \dots + \varphi^{n^2}\lambda_{n^2}$

Определение 4.13. Минимальным многочленом линейного оператора называется аннулирующий многочлен минимальной степени.

Утверждение 4.8. *μ_φ — минимальный многолчен линейного оператора φ. Тогда P — аннулирующий многлчен $phi \Rightarrow P \vdots \varphi$*

Доказательство. Разделим P на μ_φ с остатком $RaP = Q\mu_\varphi + R$. Тогда $P(\varphi) = Q(\varphi)\mu_\varphi(\varphi) + R(\varphi) = 0 \Rightarrow R(\varphi) = 0$. Получили противоречие, т.к. $\deg R < \deg \mu_\varphi$ □

Следствие. Минимальный многочлен определен с точностью до умножения на константу

Утверждение 4.9. $\chi_\varphi \vdots \mu_\varphi$

Следствие. Корни μ_φ являются корнями χ_φ

Теорема 4.3 (О взаимно простых делителях аннулирующих многолченов)**.** *Пусть $\varphi : V \to V$ — линейный оператор, f — аннулирующий многочлен, причем $f = f_1 \cdot f_2$, где $(f_1, f_2) = 1$. Тогда, если $V_i = \ker f_i(\varphi)$, то $V = V_1 \oplus V_2$, причем V_i инвариантно относительно φ*

Доказательство.

1. Докажем, что V_i — инвариантно относительно $f_i(\varphi)$. Заметим, что $f_i(\varphi)\varphi = \varphi f_i(\varphi) \Rightarrow$ V_i — инвариантно

2. Докажем, что $V_1 + V_2 = V$. Заметим, что $\exists u_1, u_2 : u_1 f_1 + u_2 f_2 = 1$. Но тогда $x = Ex = u_1(\varphi)f_1(\varphi)x + u_2(\varphi)f_2(\varphi) = f_1(\varphi)u_1(\varphi)x + f_2(\varphi)u_2(\varphi) = \underbrace{f_1(\varphi)x'}_{\in V_2} + \underbrace{f_2(\varphi)x''}_{\in V_1}$.

3. Докажем, что $V_1 \cap V_2 = \{0\}$. Действительно, если $a \in V_1, V_2$, то НОД$(f_1, f_2)(a) = 0 \Rightarrow Ea = 0 \Rightarrow a = 0$

□

Следствие. $\varphi : V \to V, f$ аннулирует φ. Тогда, если $f = f_1 f_2 \dots f_s$, где $(f_i, f_j) = 1 \Rightarrow V = \bigoplus_{i=1}^{s} V_i$, причем V_i — инвариантно относительно φ

Доказательство. Тут должно быть очевидное доказательство по индукции. □

4.6 Корневые подпространства

Определение 4.14. $\varphi : V \to V$ — линейный оператор. Вектор x называется корневым, если $\exists k \in \mathbb{N} : (\varphi - Ex)^k = 0$. Наименьшее k, удовлетворяющее такому уравнению называется высотой корневого вектора x

Замечание. Будем считать, что 0 — корневой вектор высоты 0, отвечающий любому $\lambda \in F$

Утверждение 4.10. *Множество всех корневых векторов для оператора φ, отвечающих λ является подпространством пространства V*

Доказательство. x_1, x_2 — корневые векторы, отвечающие числу λ высоты n, m соответственно. Заметим, что $(\varphi - \lambda E)^{n+m}(x_1 + x_2) = 0 \Rightarrow$ он тоже является корневым вектором, отвечающим тому же числу. □

Определение 4.15. Будем обозначать за V^λ корневое подпространство для φ, отвечающее числу λ

4.7 Корневые подпространства

Утверждение 4.11. $V^\lambda \neq \{0\} \Leftrightarrow \lambda$ *— собственное значение.*

Доказательство.

$\Rightarrow$ Если $V^\lambda \neq \{0\} \Rightarrow \exists y \neq 0, y \in V^\lambda$. Пусть его высота — k. Тогда $x = (\varphi - \lambda E)^{k-1} \neq 0, (\varphi - \lambda E)x = 0 \Rightarrow \lambda$ — собственное значение φ

$\Leftarrow$ Тогда существует ненулевой собственный вектор, который $\in V^\lambda$.

□

Теорема 4.4 (О свойствах корневых подпространств)**.** $\varphi : V \to V$ *— линейный оператор. Тогда*

1. V^λ *— инвариантно относительно* φ

2. *На* V^λ *оператор* φ *имеет единственное собственное значение, равное* λ

3. *Если W таково, что $V^\lambda \oplus W = V$*

Доказательство.

1. Пусть m — максимальная высота векторов из V^λ. $V^\lambda = \ker(\varphi - \lambda E)^m \Rightarrow \varphi(\varphi - \lambda E)^m = (\varphi - \lambda E)^m\varphi \Rightarrow$ по теореме о коммутирующих операторах, V^λ инвариантно относительно φ

2. От противного, пусть существует собственное значение, равное $\mu \neq \lambda$. Тогда

$$\exists x \in V : \varphi(x) \Rightarrow (\varphi - \lambda E)(x) = \mu x - \lambda x = (\mu - \lambda)x$$

$$(\varphi - \lambda E)^m(x) = (\mu - \lambda)^m x$$

□

ОН ОКОНЧАТЕЛЬНО ПОБЕДИЛ...