Лекция 22 от 22.02.2016

Деление многочленов с остатком

Пусть F — поле, $\mathbb{F}[x]$ — множество всех множеств от переменных x с коэффициентами из $\mathbb{F}$.

Теорема. *Пусть $G(x)$, $H(x) \in \mathbb{F}[x]$ — ненулевые многочлены, тогда существует единственная пара $Q(x)$, $R(x) \in \mathbb{F}(x)$ такая, что:*

1. $G(x) = Q(x) \cdot H(x) + R(x)$;
2. $\deg R(x) < \deg H(x)$ *или* $R(x) = 0$.

Доказательство. Аналогично делению рациональных чисел с остатком. □

Рассмотрим важный частный случай: $H(x) = x - a$.

Теорема (Безу). *Если $G(x)$, $Q(x) \in \mathbb{F}[x]$ — ненулевые многочлены, $a \in \mathbb{F}$, то $R = G(a)$ и $G(x) = Q(x)(x-a) + R$.*

Доказательство.

$$G(x) = Q(x) \cdot H(x) + R(x)$$
$$H(x) = (x-a) \Rightarrow \deg R < \deg(x-a) \Rightarrow \deg R = 0$$

Подставим $x = a$:

$$G(a) = Q(a)(a-a) + R = 0 + R = R \Rightarrow G(a) = R.$$

□

Теорема. *Многочлен степени n в поле комплексных чисел имеет n комплексных корней.*

Доказательство. По основной теореме алгебры каждый многочлен $G(x) \in \mathbb{C}[x]$ степени больше 1 имеет корень. Тогда $G(x) = (x - a_1)G_1(x)$, где a_1 — корень многочлена $G(x)$. В свою очередь, многочлен $G_1(x)$ также имеет корень, и тогда $G(x) = (x-a_1)G_1(x) = (x-a_1)(x-a_2)G_2(x)$. Продолжая по индукции, получаем, что $G(x) = (x-a_1)(x-a_2)\ldots(x-a_n)b_n$, где b_n — коэффициент при старшем члене. □

Также мы получаем следующее представление:

$$b_n x^n + b_{n-1}x^{n-1} + \ldots + b_0 = b_n(x-a_1)^{k_1}\ldots(x-a_s)^{k_s}$$

Определение. *Кратностью корня a_i называется число k_i такое, что в многочлене $b_n(x-a_1)^{k_1}\ldots(x-a_s)^{k_s}$ множитель $(x-a_i)$ имеет степень k_i.*

Определение. *Пусть V — конечномерное векторное пространство над полем $\mathbb{F}$. Рассмотрим линейный оператор $\varphi : V \to V$. Тогда характеристический многочлен φ имеет вид:*

$$\chi_\varphi(t) = (-1)^n \det(\varphi - tE) = (-1)^n \begin{vmatrix} a_{11}-t & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22}-t & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn}-t \end{vmatrix} =$$
$$= (-1)^n(t^n(-1)^n + \ldots) = t^n + c_{n-1}t^{n-1} + \ldots + c_0$$

Упражнение. *Доказать, что:*

$$c_{n-1} = -tr\varphi;$$
$$c_0 = (-1)^n \det\varphi.$$

Утверждение. *λ — собственное значение линейного оператора φ тогда и только тогда, когда $\chi_\varphi(\lambda) = 0$.*

Доказательство. λ — собственное значение $\Leftrightarrow \exists v \neq 0 : \varphi(v) = \lambda v \Leftrightarrow (\varphi - \lambda E)v = 0 \Leftrightarrow$ $\mathrm{Ker}\,(\varphi - \lambda E) \neq \varnothing \Leftrightarrow \det(\varphi - \lambda E) = 0 \Leftrightarrow \chi_\varphi(\lambda) = 0$. □

Утверждение. *Если $\mathbb{F} = \mathbb{C}$ и $\dim V > 0$, то любой линейный оператор имеет собственный вектор.*

Доказательство. Пусть $\varphi : V \to V$ — линейный оператор. У него существует характеристический многочлен $\chi_\varphi(x)$. Тогда по основной теореме алгебры у $\chi_\varphi(x)$ есть корень t_0 — собственное значение φ, следовательно существует и собственный вектор v_0 с собственным значением t_0. □

Пример. *Для линейного оператора $\varphi = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ (поворот на 90° градусов против часовой стрелки относительно начала координат) характеристический многочлен имеет вид $\chi_\varphi(x) = t^2 + 1$.*
При $\mathbb{F} = \mathbb{R} \Rightarrow$ собственных значений нет.
При $\mathbb{F} = \mathbb{C} \Rightarrow$ собственные значения $\pm i$.

Определение. *Пусть λ — собственное значение φ, тогда $V_\lambda = \{v \in V \mid \varphi(v) = \lambda v\}$ — собственное подпространство, то есть пространство, состоящее из собственных векторов с собственным значением λ и нуля.*

Определение. $\dim V_\lambda$ *— геометрическая кратность собственного значения λ.*

Определение. *Если k — кратность корня характеристического многочлена, то k — алгебраическая кратность корня.*

Утверждение. *Геометрическая кратность не больше алгебраической кратности.*

Доказательство. Зафиксируем базис $u_1, \ldots, u_p$ в пространстве V_λ, где $p = \dim V_\lambda$. Дополним базис $u_1, \ldots, u_p$ до базиса $u_1, \ldots, u_p, u_{p+1}, \ldots, u_n$ пространства V. Матрица линейного оператора φ будет выглядеть следующим образом:

$$A_\varphi = \left(\begin{array}{c|c} \lambda E & A \\ \hline 0 & B \end{array}\right), \quad \lambda E \in M_p,\ A \in M_{n-p}$$

Тогда характеристический многочлен будет следующим:

$$\chi_\varphi(t) = (-1)^n \det(A_\varphi - t) = \left(\begin{array}{ccc|c} \lambda - t & & 0 & \\ & \ddots & & A \\ 0 & & \lambda - t & \\ \hline & 0 & & b - tE \end{array}\right) = (-1)^n (\lambda - t)^p \dim(B - tE)$$

Как видим, $\chi_\varphi(t)$ имеет корень кратности хотя бы p, следовательно, геометрическая кратность, которая равна p по условию, точно не превосходит алгебраическую. □

Пример. *Рассмотрим линейный оператор $\varphi = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$.*

$V_2 = \langle e_1 \rangle \Rightarrow$ геометрическая кратность равна 1.
$\chi_\varphi(t) = (t-2)^2 \Rightarrow$ алгебраическая кратность равна 2.

Определение. *Пусть $U_1, \ldots, U_k \subseteq V$ — векторные пространства. Суммой нескольких пространств называется $U_1 + \ldots + U_k = \{u_1 + \ldots + u_k \mid u_i \in U_i\}$.*

Упражнение. *$U_1 + \ldots + U_k$ — подпространство.*

Определение. *Сумма пространств называется прямой, если* $u_1 + \ldots + u_k = 0$ *тогда и только тогда, когда* $u_1 = \ldots = u_k = 0$. *Обозначение:* $U_1 \oplus \ldots \oplus U_k$.

Упражнение. *Если* $v \in U_1 \oplus \ldots \oplus U_k$, *то существует единственный такой набор* $u_1 \in U_1, \ldots, u_k \in U_k$, *что* $v = u_1 + \ldots + u_k$.

Теорема. *Следующие условия эквивалентны:*

1. *Сумма* $U_1 + \ldots + U_k$ *— прямая;*
2. *Если* $\mathbb{e}_i$ *— базис* U_i, *то* $\mathbb{e} = \mathbb{e}_1 \cup \ldots \cup \mathbb{e}_k$ *— базис* $U_1 + \ldots + U_k$;
3. $\dim(U_1 + \ldots + U_k) = \dim U_1 + \ldots + \dim U_k$.

Доказательство.

(1) ⇒ (2) Пусть мы имеем прямую сумму $U_1 \oplus \ldots \oplus U_k$. Покажем, что $\mathbb{e}_1 \cup \ldots \cup \mathbb{e}_k$ — базис $U_1 \oplus \ldots \oplus U_k$.

Возьмем вектор $v \in U_1 \oplus \ldots \oplus U_k$ и представим его в виде суммы $v = u_1 + \ldots + u_k$, где $u_i \in U_i$. Такое разложение единственное, так как сумма прямая. Теперь представим каждый вектор этой суммы в виде линейной комбинации базиса соответствующего пространства:

$$v = (c_1^1 e_1^1 + \ldots + c_{s_1}^1 e_{s_1}^1) + \ldots + (c_1^k e_1^k + \ldots + c_{s_k}^k e_{s_k}^k)$$

Здесь e_j^i это j-ый базисный вектор в $\mathbb{e}_i$, базисе U_i. Соответственно, c_j^i это коэффициент перед данным вектором.

Если $\mathbb{e} \neq \mathbb{e}_1 \cup \ldots \cup \mathbb{e}_k$, то существует какая-то еще линейная комбинация вектора v через эти же векторы:

$$v = (d_1^1 e_1^1 + \ldots + d_{s_1}^1 e_{s_1}^1) + \ldots + (d_1^k e_1^k + \ldots + d_{s_k}^k e_{s_k}^k)$$

Вычтем одно из другого:

$$0 = v - v = ((d_1^1 - c_1^1)e_1^1 + \ldots + (d_{s_1}^1 - c_{s_1}^1)e_{s_1}^1) + \ldots + ((d_1^k - c_1^k)e_1^k + \ldots + (d_{s_k}^k - c_{s_k}^k)e_{s_k}^k)$$

Но по определению прямой суммы, ноль представим только как сумма нулей, то есть d_j^i должно равняться c_j^i. А это значит, что не существует никакой другой линейной комбинации вектора v. Что нам и требовалось.

(2) ⇒ (1) Пусть $\mathbb{e} = \mathbb{e}_1 \cup \ldots \cup \mathbb{e}_k$ — базис $U_1 + \ldots + U_k$. Тогда представим 0 в виде суммы векторов из данных пространств: $0 = u_1 + \ldots + u_k$, где $u_i \in U_i$. Аналогично прошлому пункту, разложим векторы по базисам:

$$0 = (c_1^1 e_1^1 + \ldots + c_{s_1}^1 e_{s_1}^1) + \ldots + (c_1^k e_1^k + \ldots c_{sk}^k e_{sk}^k)$$

Но только тривиальная комбинация базисных векторов дает ноль. Следовательно, $u_1 = \ldots = u_k = 0$, и наша сумма по определению прямая.

(2) ⇒ (3) Пусть $\mathbb{e} = \mathbb{e}_1 \cup \ldots \cup \mathbb{e}_k$ — базис $U_1 + \ldots + U_k$. Тогда:

$$\dim(U_1 + \ldots + U_k) = \dim(\mathbb{e}) = \dim(\mathbb{e}_{\mathbb{1}}) + \ldots + \dim(\mathbb{e}_{\mathbb{k}}) = \dim(U_1) + \ldots + \dim(U_k).$$

(3) ⇒ (2) Пусть $\dim(U_1 + \ldots + U_k) = \dim U_1 + \ldots + \dim U_k$.

Векторы $\mathbb{e}$ порождают сумму, следовательно, из $\mathbb{e}$ можно выделить базис суммы:

$$\dim(U_1 + \ldots + U_k) \leqslant \dim(\mathbb{e}) \leqslant \dim(\mathbb{e}_{\mathbb{1}}) + \ldots + \dim(\mathbb{e}_{\mathbb{k}}) = \dim U_1 + \ldots + \dim U_k.$$

Но по условию $\dim(U_1 + \ldots + U_k) = \dim U_1 + \ldots + \dim U_k$. Тогда $\dim(U_1 + \ldots + U_k) = \dim(\mathbb{e})$, и $\mathbb{e}$ это базис $U_1 + \ldots + U_k$.

□