По направлению к жордановой нормальной форме

В прошлой лекции мы, в частности, доказали, что симметричный (относительно положительно определённой формы) линейный оператор можно привести к диагональному виду. Сейчас мы хотим выяснить, к какому простому виду можно привести произвольный линейный оператор.

Для симметричного оператора мы нашли базис из собственных векторов. Оказывается, что это можно сделать и во многих других случаях.

Теорема 1. Пусть характеристический многочлен линейного оператора A на n-мерном пространстве имеет n различных корней. Тогда собственные векторы этого оператора образуют базис (в котором матрица оператора диагональна).

Действительно, для каждого собственного значения λ_i найдём собственный вектор e_i. Их n, поэтому достаточно проверить, что они линейно независимы. Пусть есть линейные зависимости, выберем ту из них, в которую с ненулевыми коэффициентами входит наименьшее число векторов: $\sum_k x_{i_k} e_{i_k} = 0$. Применяя к обеим частям оператор A, получаем другую линейную зависимость на те же векторы. Их линейная комбинация даст линейную зависимость с меньшим числом векторов. Противоречие.

Заметим, что в этом случае многочлен $(A-\lambda_1 E)\dots(A-\lambda_n E)$ от оператора A есть тождественно нулевой оператор, поскольку он аннулирует все базисные векторы. Этот многочлен совпадает с точностью до числового множителя с характеристическим многочленом оператора A, в который подставлен сам оператор. Оказывается, что это верно всегда, а не только когда собственные значения разные. Обозначим через $P_A(t)$ характеристический многочлен $\det(A-tE)$ оператора A.

Теорема 2. (Гамильтон–Кэли) $P_A(A) = 0$.

Неверное доказательство.

$$P_A(A) = \det(A - AE) = \det(A - A) = \det(0) = 0.$$

В чём тут проблема? В том, что мы не можем прямо подставить вместо элемента матрицы матрицу. Однако можно развить эту идею и получить доказательство.

Пусть $B = A - tE$. Эта матрица обращается в нуль, если положить $t = A$. Как выразить через неё её определитель? Мы знаем, что можно образовать присоединённую матрицу $\widehat{B}$ (через которую выражается обратная; см. лекцию про определители), и при этом произведение $B\widehat{B}$ есть диагональная матрица, у которой на диагонали стоит определитель матрицы B. Умножим это равенство на столбец, соответствующий базисному вектору e_i (того базиса, в котором записаны матрицы). Получим $B\widehat{B}e_i = \det(B)e_i$. Подставим теперь $t = A$ (тут можно уже не беспокоиться, поскольку каждую матрицу $B, \widehat{B}$ можно записать в виде $\sum t^k b_k$, где b_k — некоторые матрицы, не зависящие от t, и в такую сумму уже можно подставить матрицу A вместо t). Получим $0 = P_A(A)e_i$. Поэтому оператор $P_A(A)$ действует нулём на все базисные векторы и есть нулевой оператор.

Есть ещё разные красивые доказательства этой теоремы. Возможно, мы вернёмся к этому впоследствии.

Если V векторное пространство над полем k, а A — линейный оператор на этом векторном пространстве, то для каждого многочлена $f(t) \in k[t]$ можно очевидным образом построить оператор $f(A)$. Как говорят, получилось действие кольца многочленов (модуль над кольцом многочленов).

Определение 1. Пусть R — ассоциативное коммутативное кольцо с единицей. *Модулем* над R (R-модулем) называется абелева группа M, для которой есть отображение $R \times M \to M$, $(r, m) \mapsto rm$, такое что

- $\forall m_1, m_2 \in M, r \in R\ r(m_1 + m_2) = rm_1 + rm_2$;
- $\forall r_1, r_2 \in R, m \in M\ (r_1 + r_2)m = r_1 m + r_2 m$;
- $\forall r_1, r_2 \in R, m \in R\ r_1(r_2 m) = (r_1 r_2)m$;
- $\forall m \in M\ 1m = m$.

Пример 1. Модуль над полем — векторное пространство над этим полем. Модуль над $\mathbb{Z}$ — абелева группа. $\mathbb{C}$ — модуль над кольцом $\mathbb{R}[x]$ с действием $P(x)z = P(i)z$.

Определение 2. Модуль называется конечнопорождённым, если существует конечный набор $m_1, \dots, m_s$, такой что всякий элемент модуля есть $r_1 m_1 + \dots + r_s m_s$ для некоторых $r_1, \dots, r_s \in R$.

Пример 2. Конечнопорождённый модуль над полем — конечномерное линейное пространство над этим полем. В общем случае базиса может не быть. Рассмотрим абелеву группу $\mathbb{Z}/2\mathbb{Z}$. В ней нельзя выбрать набора линейно независимых над $\mathbb{Z}$ образующих (поскольку $2 \in \mathbb{Z}$ действует на этой группе нулём).

Мы докажем следующую теорему.

Теорема 3. Всякий конечнопорождённый модуль над кольцом главных идеалов есть прямая сумма модулей вида $R/(a_i)$, где a_i — элементы кольца R. Если потребовать, чтобы $a_1 \mid a_2 \mid \dots$, то набор таких модулей определён однозначно.

Пример 3. Рассмотрим модуль $k[t]/(t-\lambda)^n$ над кольцом $k[t]$. Оператор умножения на t в базисе $(t-\lambda)^{n-1}, \dots, (t-\lambda), 1$ имеет матрицу

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

Такую матрицу называют *жордановым блоком* $n \times n$, соответствующим числу λ.

Теорема о жордановой нормальной форме (для поля комплексных чисел) гласит, что для каждого линейного оператора найдётся базис, где его матрица имеет блочно-диагональный вид, причём блоки на диагонали — жордановы.

Эта теорема следует из теоремы о модулях над кольцами главных идеалов. Мы уже объясняли, что линейный оператор задаёт на пространстве структуру модуля над кольцом многочленов. Каждый модуль над кольцом многочленов есть прямая сумма модулей, аналогичных рассмотренному в примере. Мы выясним это в следующей лекции.