

§ 4. Характеристический многочлен

Пусть k — коммутативное кольцо и E — свободный модуль размерности n над k . Рассмотрим кольцо многочленов $k[t]$ и линейное отображение $A: E \rightarrow E$. Имеем гомоморфизм

$$k[t] \rightarrow k[A],$$

определенный как и выше, который переводит многочлен $f(t)$ в $f(A)$, и E превращается в модуль над кольцом $R = k[t]$. Пусть M — любая матрица размера $n \times n$ над R (например, матрица отображения A относительно некоторого базиса в E). *Характеристическим многочленом* $P_M(t)$ мы называем определитель

$$\det(tI_n - M),$$

где I_n — единичная матрица размера $n \times n$. Это элемент из $k[t]$. Кроме того, если N — обратимая матрица над R , то

$$\det(tI_n - N^{-1}MN) = \det(N^{-1}(tI_n - M)N) = \det(tI_n - M).$$

Следовательно, характеристический многочлен у матрицы $N^{-1}MN$ тот же самый, что и у M . Мы можем поэтому определить характеристический многочлен отображения A (и обозначить его через P_A) как характеристический многочлен любой матрицы M , ассоциированной с A относительно некоторого базиса. (В случае $E = 0$ мы по определению считаем характеристический многочлен равным 1.)

Если $\varphi: k \rightarrow k'$ — гомоморфизм коммутативных колец и M — матрица размера $n \times n$ над k , то очевидно, что

$$P_{\varphi M}(t) = \varphi P_M(t),$$

где φP_M получается из P_M применением φ к коэффициентам P_M .

Теорема 8 (Кэли — Гамильтон). $P_A(A) = 0$.

Доказательство. Пусть $\{v_1, \dots, v_n\}$ — базис E над k . Тогда

$$tv_j = \sum_{i=1}^n a_{ij}v_i,$$

где $(a_{ij}) = M$ — матрица отображения A относительно этого базиса. Пусть $B(t)$ обозначает матрицу $tI_n - M$. Очевидно, $B(t)$ — матрица с коэффициентами в $k[t]$. Пусть $\tilde{B}(t)$ — определенная в гл. XIII матрица с коэффициентами в $k[t]$, такая, что

$$\tilde{B}(t)B(t) = P_A(t)I_n.$$

Тогда

$$\tilde{B}(t) B(t) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} P_A(t)v_1 \\ \vdots \\ P_A(t)v_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

так как

$$B(t) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Следовательно, $P_A(t)E = 0$, а потому $P_A(A)E = 0$. Это означает, что $P_A(A) = 0$, что и требовалось показать.

Пусть теперь k — поле. Пусть E — конечномерное векторное пространство над k и $A \in \text{End}_k(E)$. Под *собственным вектором* w эндоморфизма A в E понимают элемент $w \in E$, такой, что существует элемент $\lambda \in k$, для которого $Aw = \lambda w$. Если $w \neq 0$, то λ определяется однозначно и называется *собственным значением* эндоморфизма A . Разумеется, различные собственные векторы могут иметь одинаковые собственные значения.

Теорема 9. *Собственные значения эндоморфизма A — это в точности корни его характеристического многочлена.*

Доказательство. Пусть λ — собственное значение. Тогда элемент $A - \lambda I$ необратим в $\text{End}_k(E)$ и, значит, $\det(A - \lambda I) = 0$. Следовательно, λ — корень P_A . Рассуждение обратимо, тем самым доказано и обратное утверждение.

Для упрощения обозначений мы часто будем писать $A - \lambda$ вместо $A - \lambda I$.

Теорема 10. *Ненулевые собственные векторы w_1, \dots, w_m отображения A , имеющие различные собственные значения, линейно независимы.*

Доказательство. Предположим, что

$$a_1 w_1 + \dots + a_m w_m = 0,$$

где $a_i \in k$, причем это самое короткое соотношение, в котором не все $a_i = 0$ (в предположении, что такое существует). Тогда $a_i \neq 0$ для всех i . Пусть $\lambda_1, \dots, \lambda_m$ — собственные значения наших векторов. Применим к предыдущему соотношению $A - \lambda_1$. Получим соотношение

$$a_2(\lambda_2 - \lambda_1)w_2 + \dots + a_m(\lambda_m - \lambda_1)w_m = 0,$$

которое короче исходного соотношения, — противоречие.

Следствие. Если A имеет n различных собственных значений $\lambda_1, \dots, \lambda_n$, принадлежащих собственным векторам v_1, \dots, v_n , и $\dim E = n$, то $\{v_1, \dots, v_n\}$ есть базис для E . Матрицей эндоморфизма A относительно этого базиса служит диагональная матрица

$$\begin{pmatrix} \lambda_1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{pmatrix}.$$

Предостережение. Не всегда верно, что существует базис E , состоящий из собственных векторов!

Замечание. Пусть k — подполе в k' . Если M — матрица над k , то мы можем определить ее характеристический многочлен как относительно k , так и относительно k' . Очевидно, что полученные таким путем характеристические многочлены равны. Пусть E — векторное пространство над k . Позже мы увидим, как расширить его до векторного пространства над k' . Всякое линейное отображение A продолжается до линейного отображения расширенного пространства, причем характеристический многочлен линейного отображения не изменяется. Действительно, если мы выберем базис E над k , то $E \approx k^{(n)}$ и $k^{(n)} \subset k'^{(n)}$ естественным образом. Таким образом, выбор базиса позволяет нам расширить векторное пространство, но создается впечатление, что результат зависит от выбора базиса. Инвариантное определение будет дано ниже.

Пусть $E = E_1 \oplus \dots \oplus E_r$ — представление E в виде прямой суммы векторных пространств над k . Пусть $A \in \text{End}_k(E)$, причем $AE_i \subset E_i$ для $i = 1, \dots, r$. Тогда A индуцирует на E_i линейное отображение A_i . Мы можем выбрать базис для E , состоящий из базисов для E_1, \dots, E_r , и тогда матрица для A будет состоять из блоков. Мы видим, таким образом, что

$$P_A(t) = \prod_{i=1}^r P_{A_i}(t).$$

Итак, характеристический многочлен мультипликативен на прямых суммах.

Наше предыдущее условие $AE_i \subset E_i$ можно также сформулировать, сказав, что E представимо как $k[A]$ -прямая сумма $k[A]$ -подмодулей или как $k[t]$ -прямая сумма $k[t]$ -подмодулей. Применим это к разложению пространства E , даваемому теоремой 6.

Теорема 11. Пусть E — конечномерное векторное пространство над полем k , $A \in \text{End}_k(E)$ и q_1, \dots, q_r — инварианты пары (E, A) . Тогда $P_A(t) = q_1(t) \dots q_r(t)$.

Доказательство. Предположим, что $E = k^{(n)}$ и что A представляется матрицей M . Мы видели, что ни инварианты, ни характеристический многочлен не изменяются, когда мы расширяем поле k до большего поля. Следовательно, мы можем считать, что поле k алгебраически замкнуто. Ввиду теоремы 6 мы можем предполагать, что M имеет единственный инвариант q . Запишем

$$q(t) = (t - a_1)^{e_1} \dots (t - a_s)^{e_s},$$

где a_1, \dots, a_s различны. Рассмотрим M как линейное отображение и разложим наше векторное пространство в прямую сумму подмодулей (над $k[t]$) с инвариантами

$$(t - a_1)^{e_1}, \dots, (t - a_s)^{e_s}$$

соответственно (это есть разложение на слагаемые, соответствующие степеням простых элементов). Для каждого из этих подмодулей мы можем выбрать базис так, чтобы матрица индуцированного линейного отображения имела форму, описанную в теореме 7, после чего непосредственно видно, что характеристический многочлен отображения, имеющего инвариант $(t - a)^e$, равен в точности $(t - a)^e$. Теорема доказана.

Следствие. Минимальный многочлен отображения A и его характеристический многочлен имеют одни и те же неприводимые множители.

Доказательство. Это вытекает из того, что в силу теоремы 6 q , есть минимальный многочлен.

Обобщим наше замечание, касающееся мультиликативности характеристического многочлена на прямых суммах.

Теорема 12. Пусть k — коммутативное кольцо, и пусть в следующей диаграмме:

$$\begin{array}{ccccccc} 0 & \rightarrow & E' & \rightarrow & E & \rightarrow & E'' \rightarrow 0 \\ & & A' \downarrow & & A \downarrow & & A'' \downarrow \\ 0 & \rightarrow & E' & \rightarrow & E & \rightarrow & E'' \rightarrow 0 \end{array}$$

строки являются точными последовательностями свободных модулей над k , имеющих конечную размерность. Пусть, далее, вертикальные отображения являются k -линейными отображениями, для которых диаграмма коммутативна. Тогда

$$P_A(t) = P_{A'}(t) P_{A''}(t).$$

Доказательство. Мы можем предполагать, что E' — подмодуль в E . Выберем базис $\{v_1, \dots, v_m\}$ для E' . Пусть $\{\bar{v}_{m+1}, \dots, \bar{v}_n\}$ — базис для E'' и v_{m+1}, \dots, v_n — элементы из E , отображающиеся на $\bar{v}_{m+1}, \dots, \bar{v}_n$ соответственно. Тогда $\{v_1, \dots, v_m, v_{m+1}, \dots, v_n\}$ будет базисом для E (доказательство такое же, как в теореме 3 из гл. III, § 5), и мы находимся в ситуации, описанной в § 1. Матрица для A имеет форму

$$\begin{pmatrix} M' & * \\ 0 & M'' \end{pmatrix},$$

где M' — матрица для A' и M'' — матрица для A'' . Взяв характеристический многочлен относительно этой матрицы, мы, очевидно, и получим наше мультиплективное свойство.

Теорема 13 *Пусть k — коммутативное кольцо, E — свободный модуль размерности n над k и $A \in \text{End}_k(E)$. Пусть*

$$P_A(t) = t^n + c_{n-1}t^{n-1} + \dots + c_0.$$

Тогда

$$\text{tr}(A) = -c_{n-1} \quad \text{и} \quad \det(A) = (-1)^n c_0.$$

Доказательство Что касается определителя, то заметим, что $P_A(0) = c_0$. Подстановка $t = 0$ в определение характеристического многочлена через определитель доказывает, что $c_0 = (-1)^n \det A$.

Перейдем к следу. Пусть M — матрица, представляющая A относительно некоторого базиса, $M = (a_{ij})$. Рассмотрим определитель $\det(tI_n - a_{ij})$. В его разложении по первому столбцу содержится диагональный член

$$(t - a_{11}) \dots (t - a_{nn}),$$

который вносит в коэффициент при t^{n-1} вклад, равный

$$-(a_{11} + \dots + a_{nn}).$$

Никакой другой член в этом разложении ничего не добавляет к коэффициенту при t^{n-1} , так как степень t , встречающаяся в других членах, не превосходит t^{n-2} . Это доказывает наше утверждение, касающееся следа.

Следствие. *Пусть обозначения те же, что и в теореме 12. Тогда*

$$\text{tr}(A) = \text{tr}(A') + \text{tr}(A'') \quad \text{и} \quad \det(A) = \det(A') \det(A'').$$

Доказательство. Очевидно.

Дадим теперь нашим результатам интерпретацию в терминах группы Эйлера — Гроененка.

Пусть k — коммутативное кольцо. Рассмотрим категорию, объектами которой являются пары (E, A) , где E — k -модуль и $A \in \text{End}_k(E)$. Определим морфизм

$$(E', A') \rightarrow (E, A)$$

как k -линейное отображение $E' \xrightarrow{k} E$, для которого коммутативна следующая диаграмма:

$$\begin{array}{ccc} E' & \xrightarrow{f} & E \\ A' \downarrow & & \downarrow A \\ E' & \xrightarrow{f} & E \end{array}$$

Мы можем определить ядро такого морфизма снова как пару. Действительно, пусть E'_0 — ядро $f: E' \rightarrow E$. Тогда A' отображает E'_0 в себя, так как $fA'E'_0 = AfE'_0 = 0$. Пусть A'_0 — ограничение A' на E'_0 . Пары (E'_0, A'_0) по определению является ядром нашего морфизма.

Будем обозначать по-прежнему через f морфизм пары $(E', A') \rightarrow (E, A)$. Мы можем говорить о точной последовательности

$$(E', A') \rightarrow (E, A) \rightarrow (E'', A''),$$

понимая под этим, что точна индуцированная последовательность

$$E' \rightarrow E \rightarrow E''.$$

Мы будем также писать 0 вместо $(0, 0)$ в соответствии с нашим общим соглашением использовать символ 0 для всех тех вещей, которые ведут себя подобно нулевому элементу.

Заметим, что наши пары ведут себя теперь формально как модули и что они фактически образуют абелеву категорию.

Пусть k — поле, и пусть \mathcal{A} состоит из всех пар (E, A) , где E имеет конечную размерность над k . Тогда *теорема 12 утверждает, что характеристический многочлен является отображением Эйлера — Пуанкаре, определенным для всякого объекта из нашей категории \mathcal{A} , со значениями в мультипликативном моноиде многочленов со старшим коэффициентом 1*. Так как значения этого отображения лежат в моноиде, то здесь используется несколько более общее понятие, чем введенное в гл. IV, где мы брали значения в группе. Разумеется, когда k есть поле, что наиболее часто встречается в приложениях, мы можем считать, что значения нашего отображения лежат в мультипликативной группе отличных от нуля рациональных функций, так что применимы наши предыдущие рассмотрения.

Аналогичное замечание справедливо также для следа и определителя. Если k — поле, то след есть отображение Эйлера в аддитивную группу поля, а определитель — отображение Эйлера

в мультиликативную группу поля¹⁾. Отметим также, что все эти отображения (подобно всем отображениям Эйлера) определены на классах пар относительно изоморфизма и что они определены на группе Эйлера — Гrotендика.

Теорема 14. Пусть k — целостное кольцо, M — матрица размера $n \times n$ над k и f — многочлен из $k[t]$. Предположим, что $P_M(t)$ имеет разложение

$$P_M(t) = \prod_{i=1}^n (t - a_i)$$

на линейные множители над k . Тогда характеристический многочлен матрицы $f(M)$ задается формулой

$$P_{f(M)}(t) = \prod_{i=1}^n (t - f(a_i))$$

и

$$\text{tr}(f(M)) = \sum_{i=1}^n f(a_i), \quad \det(f(M)) = \prod_{i=1}^n f(a_i).$$

Доказательство. Допустим сначала, что k — поле. Тогда, используя каноническое разложение на блоки, описанное в теореме 7 § 3, мы обнаруживаем, что наше утверждение совершенно очевидно. В случае когда k — кольцо, используем стандартный прием с подстановкой. Для этого, однако, необходимо знать, что если $X = (x_{ij})$ — матрица с алгебраически независимыми элементами над \mathbf{Z} , то $P_X(t)$ имеет n различных корней y_1, \dots, y_n [в алгебраическом замыкании поля $\mathbf{Q}(X)$], и что существует гомоморфизм

$$\mathbf{Z}[x_{ij}, y_1, \dots, y_n] \rightarrow k,$$

отображающий X на M и y_1, \dots, y_n на a_1, \dots, a_n . Но это очевидно для читателя, который прочитал главу о целых расширениях колец, а читатель, который этого не сделал, может забыть об этой части теоремы²⁾.

УПРАЖНЕНИЯ

1. Пусть T — верхняя треугольная квадратная матрица над коммутативным кольцом (т. е. все элементы под диагональю и на ней равны 0). Показать, что T нильпотентна.

¹⁾ Точнее, в мультиликативную полугруппу, так как значение определителя может быть равно нулю. — Прим. ред.

²⁾ Проще вложить k в поле частных. — Прим. ред.

2. Провести непосредственно доказательство того факта, что определитель матрицы

$$\begin{pmatrix} M_1 & & * & * \\ 0 & M_2 & & * \\ 0 & 0 & \ddots & \\ \vdots & \vdots & \ddots & \ddots \\ 0 & 0 & \dots & 0 & M_s \end{pmatrix},$$

где каждая M_i — квадратная матрица, равен произведению определителей матриц M_1, \dots, M_s .

3. Пусть k — коммутативное кольцо и M, M' — квадратные матрицы размера $n \times n$ над k . Показать, что характеристические многочлены матриц MM' и $M'M$ равны.

4. Показать, что собственные значения матрицы

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

в поле комплексных чисел равны $\pm 1, \pm i$.

5. Пусть M, M' — квадратные матрицы над полем k . Пусть соответственно q, q' — их минимальные многочлены. Показать, что минимальный многочлен матрицы

$$\begin{pmatrix} M & 0 \\ 0 & M' \end{pmatrix}$$

равен наименьшему общему кратному q, q' .

6. Пусть A — nilпотентный эндоморфизм конечномерного векторного пространства E над полем k . Показать, что $\text{tr}(A) = 0$.

7. Пусть R — целостное кольцо главных идеалов, E — свободный модуль размерности n над R и $E^* = \text{Hom}_R(E, R)$ — его дуальный модуль. Тогда E^* — свободный модуль размерности n . Пусть F — подмодуль в E . Показать, что E^*/F^\perp можно рассматривать как подмодуль в F^* и что его инварианты те же самые, что и инварианты F в E .

8. Пусть E — конечномерное векторное пространство над полем k и $A \in \text{Aut}_k(E)$. Показать, что следующие условия эквивалентны:

(i) $A = I + N$, где N — nilпотентный эндоморфизм

(ii) Существует базис для E , такой, что у матрицы эндоморфизма A относительно этого базиса все диагональные элементы равны 1, а все элементы над диагональю равны 0.

(iii) Все корни характеристического многочлена эндоморфизма A (в алгебраическом замыкании поля k) равны 1.

9. Пусть k — поле характеристики 0 и M — матрица размера $n \times n$ над k . Показать, что M nilпотентна в том и только в том случае, если $\text{tr}(M^v) = 0$ для $1 \leq v \leq n$.

10. Обобщить теорему 14 на рациональные функции (вместо многочленов), предполагая, что k — поле.

11. Пусть E — конечномерное пространство над полем k , $a \in k$ и E_a — подпространство в E , порожденное всеми собственными векторами данного эндоморфизма A пространства E , имеющими a в качестве собственного значения. Показать, что всякий ненулевой элемент из E_a является собственным вектором эндоморфизма A с собственным значением a .

12. Пусть E — конечномерное пространство над полем k , $A \in \text{End}_k(E)$ — собственный вектор для A . Пусть элемент $B \in \text{End}_k(E)$ таков, что $AB = BA$. Показать, что Bv — также собственный вектор для A (если $Bv \neq 0$) с тем же собственным значением и что в случае алгебраически замкнутого поля k эндоморфизмы A и B имеют общий собственный вектор.

Диагонализируемые эндоморфизмы. Пусть E — конечномерное векторное пространство над полем k , $S \in \text{End}_k(E)$. Мы говорим, что эндоморфизм S — *диагонализируемый*, если существует базис для E , состоящий из собственных векторов S . Матрица эндоморфизма S относительно этого базиса является диагональной матрицей.

13. (а) Если эндоморфизм S диагонализируем, то его минимальный многочлен над k имеет вид $q(t) = \prod_{i=1}^m (t - \lambda_i)$, где $\lambda_1, \dots, \lambda_m$ — различные элементы из k .

(б) Обратно, если минимальный многочлен для S имеет предыдущий вид, то эндоморфизм S диагонализируем. [Указание: пространство может быть разложено в прямую сумму подпространств $E\lambda_i$, анулируемых эндоморфизмами $S - \lambda_i$.]

(в) Показать, что если эндоморфизм S диагонализируем и F — такое подпространство в E , что $SF \subset F$, то S диагонализируем также как эндоморфизм F , т. е. что F имеет базис, состоящий из собственных векторов S .

(г) Пусть S, T — эндоморфизмы E . Предположим, что S, T коммутируют. Предположим также, что и S , и T оба диагонализируемы. Показать, что они одновременно диагонализируемы, т. е. что существует базис для E , состоящий из векторов, собственных как для S , так и для T . [Указание: если λ — собственное значение эндоморфизма S и E_λ — подпространство в E , состоящее из всех векторов v , таких, что $Sv = \lambda v$, то $TE_\lambda \subset E_\lambda$.]

14. Пусть E — конечномерное векторное пространство над алгебраически замкнутым полем k , $A \in \text{End}_k(E)$. Показать, что эндоморфизм A может быть единственным образом записан в виде суммы

$$A = S + N,$$

где S диагонализируем, N нильпотент и $SN = NS$. Показать, что S, N могут быть представлены в виде многочленов от A . [Указание: пусть $P_A(t) = \prod (t - \lambda_i)^{m_i}$ — разложение $P_A(t)$ с различными λ_i ; E_i — ядро $(A - \lambda_i)^{m_i}$. Тогда E — прямая сумма E_i . Определить S на E так, что на всяком E_i будет $Sv = \lambda_i v$ для всех $v \in E_i$. Положить $N = A - S$. Показать, что S, N удовлетворяют нашим требованиям. Чтобы представить S в виде многочлена от A , рассмотреть многочлен $g(t) = \sum \lambda_i g_i(t)$, где многочлены $g_i(t)$ выбраны так, что для всякого i компонента в E_i любого элемента $v \in E$ равна $g_i(A)v$. Тогда $S = g(A)$ и $N = A - g(A)$.]

15. После того как вы прочтете параграф о тензорных произведениях векторных пространств, вы легко сможете сделать следующее упражнение. Пусть E, F — конечномерные векторные пространства над алгебраически

замкнутым полем k , $A: E \rightarrow E$ и $B: F \rightarrow F$ — k -эндоморфизмы пространств E, F соответственно. Пусть

$$P_A(t) = \prod (t - a_i)^{n_i} \quad \text{и} \quad P_B(t) = \prod (t - b_j)^{m_j}$$

— разложения их характеристических многочленов на различные линейные множители. Тогда

$$P_{A \otimes B}(t) = \prod_{i,j} (t - a_i b_j)^{n_i m_j}.$$

[Указание: разложить E в прямую сумму подпространств E_i , где E_i — подпространство, аннулируемое некоторой степенью $A - a_i$. То же самое сделать с F и получить разложение в прямую сумму подпространств F_j . Затем показать, что некоторая степень эндоморфизма $A \otimes B - a_i b_j$ аннулирует $E_i \otimes F_j$. Использовать тот факт, что $E \otimes F$ есть прямая сумма подпространств $E_i \otimes F_j$ и что $\dim_k(E_i \otimes F_j) = n_i m_j$.]

16. Пусть Γ — свободная абелева группа размерности $n \geq 1$, Γ' — ее подгруппа, имеющая также размерность n . Пусть $\{v_1, \dots, v_n\}$ — базис Γ и $\{w_1, \dots, w_n\}$ — базис Γ' . Запишем

$$w_i = \sum a_{ij} v_j$$

Показать, что индекс $(\Gamma : \Gamma')$ равен абсолютной величине определителя матрицы (a_{ij}) .

17. Доказать теорему о нормальном базисе для конечного расширения конечного поля.

18. Пусть $A = (a_{ij})$ — квадратная матрица размера $n \times n$ над коммутативным кольцом k , A_{ij} — матрица, полученная вычеркиванием i -й строки и j -го столбца из A . Пусть $b_{ij} = (-1)^{i+j} \det(A_{ij})$ и B — матрица (b_{ij}) . Показать, что $\det(B) = \det(A)^{n-1}$, сведя задачу к случаю, когда A — матрица с переменными коэффициентами над кольцом целых чисел. Использовать тот же метод для получения другого доказательства теоремы Гамильтона — Кэли о том, что $P_A(\bar{A}) = 0$.

19. Пусть (E, A) и (E', A') — пары, состоящие из конечномерного векторного пространства над некоторым полем k и k -эндоморфизма. Показать, что эти пары изоморфны в том и только в том случае, если их инварианты равны.