§ 3. *Разложение над одним эндоморфизмом*

Пусть k — поле и E — конечномерное векторное пространство над k, $E \neq 0$. Пусть $A \in \operatorname{End}_k(E)$ — линейное отображение E в себя, t — трансцендентный элемент над k. Определим некоторое представление кольца многочленов $k[t]$ в E. А именно: имеет место гомоморфизм

$$k[t] \to k[A] \subset \operatorname{End}_k(E),$$

который получается подстановкой A вместо t в многочлены. Кольцо $k[A]$ является подкольцом в $\operatorname{End}_k(E)$, порожденным A, и притом коммутативным, так как степени A коммутируют друг с другом. Таким образом, если $f(t)$ — многочлен и $v \in E$, то

$$f(t)v = f(A)v.$$

Ядро гомоморфизма $f(t) \mapsto f(A)$ есть главный идеал в $k[t]$, который $\neq 0$, поскольку $k[A]$ конечномерно над k. Он порождается однозначно определенным многочленом степени >0 со старшим коэффициентом 1. Этот многочлен будет называться *минимальным многочленом* эндоморфизма A над k и будет обозначаться через $q_A(t)$. Разумеется, он не обязательно неприводим.

Предположим, что существует элемент $v \in E$, *такой, что* $E = k[t]v = k[A]v$. Это означает, что E порождается над полем k элементами

$$v,\ Av,\ A^2v,\ \ldots .$$

Мы назвали такие модули *главными*. Можно записать $E = Rv = (v)$, где $R = k[t]$.

Если $q_A(t) = t^d + a_{d-1}t^{d-1} + \ldots + a_0$, то элементы

$$v,\ Av,\ \ldots,\ A^{d-1}v$$

образуют базис для E над k. Это доказывается точно так же, как и аналогичное утверждение для конечных расширений полей. Во-первых, отметим, что они линейно независимы, так как любое соотношение линейной зависимости над k давало бы многочлен $g(t)$ меньшей степени, чем $\deg q_A$, и такой, что $g(A) = 0$. Во-вторых, они порождают E, так как любой многочлен $f(t)$ может быть записан в виде $f(t) = g(t)q_A(t) + r(t)$, где $\deg r < \deg q_A$. Следовательно, $f(A) = r(A)$.

Ясно, что относительно этого базиса матрица эндоморфизма A имеет следующий вид:

$$\begin{pmatrix} 0 & 0 & 0 \ldots 0 & -a_0 \\ 1 & 0 & 0 \ldots 0 & -a_1 \\ 0 & 1 & 0 \ldots 0 & -a_2 \\ \cdot & \cdot & \cdot \quad \cdot \quad \cdot & \cdot \\ 0 & 0 & 0 \quad\ \ 0 & -a_{d-2} \\ 0 & 0 & 0 \ldots 1 & -a_{d-1} \end{pmatrix}.$$

Если модуль E главный, то E изоморфен фактормодулю $k[t]/q_A(t)$ относительно отображения $f(t) \longmapsto f(A)v$. Многочлен q_A однозначно определен эндоморфизмом A и не зависит от выбора образующей v модуля E. Это по существу очевидно, так как если f_1, f_2 — два многочлена со старшим коэффициентом 1, то модуль $k[t]/f_1(t)$ тогда и только тогда изоморфен $k[t]/f_2(t)$, когда $f_1 = f_2$.

Если модуль E главный, то мы будем называть q_A *полиномиальным инвариантом* E относительно A, или просто *инвариантом*.

Теорема 6. *Пусть E — ненулевое конечномерное пространство над полем k, и пусть $A \in \mathrm{End}_k(E)$. Тогда E обладает разложением в прямую сумму*

$$E = E_1 \oplus \ldots \oplus E_r,$$

где каждое слагаемое E_i является главным $k[A]$-подмодулем с инвариантом $q_i \neq 0$, причем

$$q_1 \mid q_2 \mid \ldots \mid q_r.$$

Последовательность $(q_1, \ldots, q_r)$ однозначно определяется пространством E и эндоморфизмом A, и q_r есть минимальный многочлен для A.

Доказательство. Первое утверждение есть просто перефразировка на другом языке структурной теоремы для модулей над кольцами главных идеалов. Далее, ясно, что $q_r(A) = 0$, так как $q_i \mid q_r$ для всякого i. Никакой многочлен меньшей степени, чем q_r, не может аннулировать E, поскольку, в частности, такой многочлен не аннулирует E_r. Таким образом, q_r — минимальный многочлен.

Мы будем называть $(q_1, \ldots, q_r)$ *инвариантами* пары (E, A). Пусть $E = k^{(n)}$, и пусть A — матрица размера $n \times n$, которую мы можем рассматривать как линейное отображение E в себя. Инварианты $(q_1, \ldots, q_r)$ этого линейного отображения будут называться *инвариантами* матрицы A (над k).

Следствие 1. *Пусть k' — расширение поля k и A — матрица размера $n \times n$ над k. Инварианты матрицы A над k те же самые, что и ее инварианты над k'.*

Доказательство. Пусть $\{v_1, \ldots, v_n\}$ — базис $k^{(n)}$ над k. Тогда мы можем рассматривать его также как базис $k'^{(n)}$ над k'. (Единичные векторы лежат в k-пространстве, порожденном элементами $v_1, \ldots, v_n$; следовательно, $v_1, \ldots, v_n$ порождают n-мерное пространство $k'^{(n)}$ над k'.) Пусть $E = k^{(n)}$ и L_A (соответственно L'_A) — линейное отображение пространства E (соответственно $k'^{(n)}$), определенное матрицей A. Матрица отображения L_A относительно нашего заданного базиса совпадает с матрицей отображения L'_A. Мы можем выбрать базис, который соответствует разложению

$$E = E_1 \oplus \ldots \oplus E_r,$$

определенному инвариантами $q_1, \ldots, q_r$. Отсюда вытекает, что инварианты не изменятся, когда мы поднимем этот базис до базиса $k'^{(n)}$.

Следствие 2. *Пусть A, B — матрицы размера $n \times n$ над полем k и k' — расширение k. Предположим, что существует обратимая матрица C' над k', такая, что $B = C'AC'^{-1}$. Тогда существует обратимая матрица C над k, такая, что $B = CAC^{-1}$.*

Доказательство. Упражнение.

Структурная теорема для модулей над кольцами главных идеалов дает нам два типа разложений. Один — в соответствии с инвариантами, как в предыдущей теореме. Другой — в соответствии со степенями простых элементов.

Пусть $E \neq 0$ — конечномерное векторное пространство над полем k и A: $E \to E$ — эндоморфизм из $\operatorname{End}_k(E)$. Пусть $q = q_A$ — его минимальный многочлен. Тогда q имеет разложение

$$q = p_1^{e_1} \ldots p_s^{e_s} \qquad (e_i \geqslant 1)$$

в произведение степеней (различных) простых элементов. Следовательно, E есть прямая сумма подмодулей

$$E = E(p_1) \oplus \ldots \oplus E(p_s),$$

где каждый $E(p_i)$ аннулируется многочленом $p_i^{e_i}$. Кроме того, каждый такой подмодуль может быть представлен в виде прямой суммы подмодулей, изоморфных $k[t]/p^e$ для некоторого неприводимого многочлена p и некоторого целого числа $e \geqslant 1$.

Теорема 7. *Пусть $q_A(t) = (t - \alpha)^e$ для некоторого $\alpha \in k$, $e \geqslant 1$. Предположим, что E изоморфно $k[t]/(q)$. Тогда E имеет базис над k, такой, что относительно этого базиса матрица эндоморфизма A имеет вид*

$$\begin{pmatrix} \alpha & 0 & \ldots & 0 \\ 1 & \alpha & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & & \cdot & \cdot \\ \cdot & & \cdot\ \cdot & \cdot \\ 0 & \ldots & 1 & \alpha \end{pmatrix}$$

Доказательство. Так как E изоморфно $k[t]/q$, то существует элемент $v \in E$, такой, что $k[t]v = E$. Этот элемент соответствует единичному элементу кольца $k[t]$ при изоморфизме

$$k[t]/q \to E.$$

Мы утверждаем, что элементы

$$v,\ (t-\alpha)v,\ \ldots,\ (t-\alpha)^{e-1}v,$$

или, что эквивалентно,

$$v,\ (A-\alpha)v,\ \ldots,\ (A-\alpha)^{e-1}v,$$

образуют базис для E над k. Они линейно независимы над k, так как любое соотношение линейной зависимости давало бы соотношение линейной зависимости между

$$v,\ Av,\ \ldots,\ A^{e-1}v$$

и, следовательно, давало бы многочлен $g(t)$ степени, меньшей, чем $\deg q$, такой, что $g(A)=0$. Так как $\dim E = e$, то отсюда следует, что наши элементы образуют базис для E над k. Но $(A-\alpha)^e = 0$. Ясно, что матрица эндоморфизма A относительно этого базиса имеет форму, указанную в нашей теореме.

Следствие. *Пусть k — алгебраически замкнутое поле, E — конечномерное ненулевое векторное пространство над k и $A \in \mathrm{End}_k(E)$. Тогда существует базис пространства E над k, такой, что матрица эндоморфизма A относительно этого базиса состоит из блоков, каждый из которых имеет вид, описанный в теореме.*

О матрице, имеющей форму, описанную в предыдущем следствии, говорят, что она имеет *жорданову каноническую форму*.

Замечание. Матрица (или эндоморфизм) N называется *нильпотентной*, если существует целое число $d > 0$, такое, что $N^d = 0$. Мы видим, что в теореме 7 или ее следствии матрица M записывается в виде

$$M = B + N,$$

где матрица N нильпотентна. Действительно, N есть треугольная матрица (т. е. она имеет нулевые коэффициенты на и над диагональю) и B—диагональная матрица, диагональные элементы которой являются корнями минимального многочлена. Такое разложение может быть получено всякий раз, когда поле k таково, что все корни минимального многочлена лежат в k. Отметим также, что единственным случаем, когда матрица N будет нулевой, будет тот, когда все корни минимального многочлена имеют кратность 1. В этом случае матрица M является диагональной матрицей с n различными элементами диагонали, где $n = \dim E = \deg q_A$.