

ЛЕКЦИЯ 10

В этой лекции R — произвольное кольцо (как всегда коммутативное, ассоциативное и с единицей).

Определение 1. Многочлен $p(x) \in R[x]$ называется *унитальным*, если его старший коэффициент равен 1.

Теорема 1 (Гамильтон–Кэли). Пусть R — кольцо, $I \triangleleft R$, M — R -модуль, порождённый n образующими, φ — эндоморфизм M , такой что $\varphi(M) \subseteq IM$. Тогда существует унитарный многочлен $p(x) = x^n + p_1x^{n-1} + \dots + p_n$, где $p_j \in I^j$, такой что $p(\varphi) = 0$.

Частный случай: Если $R = F$ — поле, $I = F$, M — n -мерное векторное пространство, φ — линейный оператор, то теорема Гамильтона–Кэли утверждает, что существует унитарный многочлен $p(x)$ степени n (характеристический), который аннулирует φ , то есть $p(\varphi) = 0$.

Доказательство. Пусть $m_1, \dots, m_n$ — порождающие элементы модуля M как R -модуля. Так как $\varphi(M) \subseteq IM$, то для каждого i :

$$\varphi(m_i) = \sum_{j=1}^n a_{ij}m_j, \quad \text{где } a_{ij} \in I.$$

На M можно задать структуру $R[x]$ -модуля, определив действие

$$x \cdot m := \varphi(m)$$

для любого $m \in M$. Рассмотрим вектор $\vec{m} = \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$ и матрицу $A = (a_{ij})$.

Тогда:

$$x \cdot \vec{m} = A\vec{m}.$$

Рассмотрим матричное уравнение, полученное из соотношения $(x \cdot E - A)\vec{m} = 0$:

$$(x \cdot E - A) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0,$$

Умножим это уравнение слева на присоединённую матрицу. По свойству присоединённой матрицы получаем:

$$\det(x \cdot E - A) \cdot E \cdot \vec{m} = 0 \iff \det(x \cdot E - A)m_j = 0 \quad \text{для всех } j = 1, \dots, n.$$

Тогда $p(x) = \det(x \cdot E - A)$ аннулирует весь модуль M . Очевидно, что $p(x)$ — унитарный многочлен. Из построения следует, что $p(\varphi)$ является нулевым эндоморфизмом. Матрица $x \cdot E - A$ имеет вид:

$$x \cdot E - A = \begin{pmatrix} x - a_{11} & -a_{12} & \dots & -a_{1n} \\ -a_{21} & x - a_{22} & \dots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \dots & x - a_{nn} \end{pmatrix}$$

Коэффициент p_k при x^k в определителе $p(x)$ (для $k < n$) получается как сумма произведений, в которых $n - k$ элементов взяты вне главной диагонали

матрицы A . Поскольку элементы a_{ij} принадлежат идеалу I , эти произведения принадлежат идеалу I^{n-k} , то есть $p_{n-k} \in I^{n-k}$. $\square$

Следствие 1. Пусть R — кольцо, M — конечно порождённый R -модуль.

- а) $\alpha : M \rightarrow M$ — эпиморфизм $\Rightarrow \alpha$ является изоморфизмом.
- б) Если M — свободный модуль ранга n ($M \cong R^n$), то любая система порождающих этого модуля из n элементов является базисом модуля M .
- в) Ранг свободного модуля определяется однозначно (доказательство для модулей конечного ранга).

Доказательство. (а) Рассмотрим M как $R[t]$ -модуль с действием

$$t \cdot m := \alpha(m).$$

Рассмотрим идеал $I = (t) \triangleleft R[t]$. Так как α -эпиморфизм, получаем

$$tM = \alpha(M) = M.$$

Рассмотрим эндоморфизм $\varphi = \text{id}$. Тогда $\varphi(M) = M$. Так как $\varphi(M) \subseteq IM = M$, по теореме Гамильтона–Кэли существует унитарный многочлен

$$p(x) = x^n + p_1 x^{n-1} + \dots + p_n,$$

где $p_j \in I^j = (t^j)$, такой что $p(\text{id}) = 0$. Многочлен $p = p(x, t) \in (R[t])[x]$ имеет вид

$$p(x, t) = x^n + s_1(t)x^{n-1} + \dots + s_n(t), \quad \text{где } s_j(t) = t^j \cdot \tilde{s}_j(t) \quad \forall j.$$

Подставляя $x = \text{id}$ и $t = \alpha$, получаем:

$$p(\text{id}, \alpha) = \text{id} + \alpha \cdot \tilde{q}(\alpha) = 0.$$

Соотношение $\tilde{q}(\alpha) \cdot \alpha = -\text{id}$ означает, что α обратим, то есть является изоморфизмом.

(б) Пусть $M \cong R^n$. Это означает, что существует изоморфизм $\gamma : M \rightarrow R^n$. Пусть $m_1, \dots, m_n$ — образующие элементы M . Рассмотрим эпиморфизм $\beta : R^n \rightarrow M$, определённый по правилу $(r_1, \dots, r_n) \mapsto \sum r_i m_i$. Тогда отображение $\beta \circ \alpha : M \rightarrow M$ является эпиморфизмом. По пункту (а) получаем, что $\beta \circ \alpha$ — изоморфизм. Следовательно, β — изоморфизм ($\beta^{-1} = \alpha \circ (\beta \circ \alpha)^{-1}$). Получили $\text{Ker} \beta = \{0\}$, значит из равенства $\sum r_i m_i = 0$ следует все $r_i = 0$. Следовательно, $m_1, \dots, m_n$ — базис модуля M .

(в) Предположим противное: пусть $R^n \cong R^m$, и пусть $m < n$. Пусть $e_1, \dots, e_m$ — базис R^m . Рассмотрим элементы $(e_1, \dots, e_m, 0, \dots, 0)$ (где нулей $n - m$ штук). Это система образующих. По пункту (б) это базис в R^n , противоречие с тем, что данная система очевидно линейно зависима. $\square$

Предложение 1. Пусть R — кольцо, $J \triangleleft R[x]$, $S = R[x]/J$. Обозначим $s = x + J$. Тогда:

- а) Кольцо S порождено как R -модуль $\leq n$ элементами тогда и только тогда, когда J содержит унитарный многочлен степени $\leq n$.
В этом случае образующие S как R -модуля — это $s^0, s^1, s^2, \dots, s^{n-1}$.
- б) S является конечно порождённым свободным R -модулем тогда и только тогда, когда J порождён одним унитарным многочленом степени n .
В этом случае, система образ. $s^0, s^1, s^2, \dots, s^{n-1}$ — базис.

Доказательство. $R[x]$ порождается элементами x^k $k \in \mathbb{N} \cup \{0\}$ как R -модуль. Следовательно, S порождается $1, s, \dots, s^k, \dots$ как R -модуль.

(а) $\Leftarrow$ Пусть J содержит унитарный многочлен $p(x) = x^n + r_{n-1}x^{n-1} + \dots + r_0$. Тогда в S выполняется соотношение:

$$s^n = -r_{n-1}s^{n-1} - \dots - r_0.$$

Пусть $k \geq n$, тогда

$$s^k = -r_{n-1}s^{k-1} - \dots - r_0s^{k-n}.$$

Следовательно, любой элемент s^k при $k \geq n$ выражается через $1, s, \dots, s^{k-1}$. Значит, S порождён как R -модуль элементами $1, s, \dots, s^{n-1}$ то есть $\leq n$ элементами.

$\Rightarrow$ S порождён $m_1, \dots, m_n$. Определим эндоморфизм φ модуля S по правилу $\varphi(\tilde{s}) := s \cdot \tilde{s}$. Положим $I = R$ и применим теорему Гамильтона-Кэли. Получим, что существует унитарный многочлен p степени n такой, что $p(\varphi) = 0$. Имеем $p(\varphi)(1) = p(s) \cdot 1 \Rightarrow p(s) = 0$. Следовательно, $p(x) \in J$.

(б) $\Rightarrow$ Пусть $J = (p(x))$, где $p(x)$ — унитарный многочлен степени n . Тогда из пункта а) S порождён как R -модуль элементами $1, s, \dots, s^{n-1}$. Покажем, что это базис.

Действительно, пусть $\sum_{i=0}^{n-1} a_i s^i = 0$, где $a_i \in R$. Рассмотрим многочлен $q(x) = \sum_{i=0}^{n-1} a_i x^i$. Тогда $q(s) = 0$, значит, $q(s) \in J = (p(x))$. Следовательно, $p(x) \mid q(x)$. Но $\deg q \leq n-1 < \deg p$, поэтому $q(x) = 0$, то есть все $a_i = 0$.

Замечание 1. Тут используется, что многочлен p унитарный. Вообще говоря, для колец с делителями нуля ступень произведения многочленов может быть меньше суммы степеней. Но если один из старших коэффициентов равен единице, то такого не может случиться.

Значит, $1, s, \dots, s^{n-1}$ — линейно независимы. Они также порождают S . Следовательно, $1, s, \dots, s^{n-1}$ — базис S как R -модуля.

$\Leftarrow$ Пусть S — свободный R -модуль. Тогда $S \cong R^n$, следовательно, S порождён n элементами. Из пункта а) следует, что существует унитарный многочлен $p(x)$ степени $\deg p(x) \leq n$, содержащийся в идеале J . На самом деле, степень $p(x)$ равна n (иначе S будет порождён меньшим числом элементов, что противоречит корректности ранга). Тогда S как R -модуль порождён элементами $1, s, \dots, s^{n-1}$. По следствию 1 элементы $1, s, \dots, s^{n-1}$ образуют базис S как R -модуля.

Докажем, что $J = (p(x))$ от противного: пусть $f(x) \in J$ и $f(x) = q(x)p(x) + r(x)$, где $\deg r < \deg p$. Это корректно, так как $p(x)$ — унитарный многочлен. Поскольку $f(x) \in J$ и $p(x) \in J$, то $r(x) = f(x) - q(x)p(x)$ также принадлежит J .

Так как $r(x) \in J$, имеем $r(s) = 0$. Учитывая, что $\deg r < \deg p = n$, это означает, что $r(s) = 0$ является линейной зависимостью на базисных элементах $1, s, \dots, s^{n-1}$. Противоречие. Значит, $r(x) = 0$. Таким образом, $f(x) = q(x)p(x)$, то есть $J = (p(x))$. $\square$

Определение 2. Пусть R — подкольцо кольца S , $S \supseteq R$. Будем говорить, что S — R -алгебра.

Определение 3. Элемент $s \in S$ является *целым над R* , если существует унитарный многочлен $p(x) \in R[x]$ такой, что $p(s) = 0$.

S — *цела над R* , если каждый элемент $s \in S$ целый над R .

Определение 4. S называется *конечной над R* , если это конечно порождённый R -модуль.

Следствие 2. Пусть S — R -алгебра. Тогда S — конечно порождённый R -модуль тогда и только тогда, когда S порождена конечным числом целых элементов (как R -алгебра).

Доказательство. $\Rightarrow$ Пусть $m_1, \dots, m_n$ — образующие S как R -модуля. Рассмотрим $s \in S$. Определим эндоморфизм $\varphi(\tilde{s}) := s \cdot \tilde{s}$. По теореме Гамильтона–Кэли для $I = R$ и $M = S$, существует унитарный многочлен $p(x)$ такой, что $p(\varphi) = 0$. Тогда $p(\varphi)(\tilde{s}) = 0$. В частности, для $\tilde{s} = 1$:

$$p(\varphi)(1) = p(s) \cdot 1 = 0 \Rightarrow p(s) = 0.$$

Таким образом, $\forall$ элемент s целый над R . Следовательно, $m_1, \dots, m_n$ — целые и порождают S как R -алгебру.

$\Leftarrow$

Пусть S порождена как R -алгебра элементами $s_1, \dots, s_k$ — целыми над R . Рассмотрим последовательность расширений:

$$R \subseteq R[s_1] \subseteq R[s_1, s_2] \subseteq \dots \subseteq R[s_1, \dots, s_k] = S.$$

$R[s_1]$ — конечно порождённый R -модуль, так как $R[s_1] \cong R[x]/\mathcal{J}$, где $\mathcal{J} = (p_1(x))$, и $p_1(x)$ — унитарный (поскольку s_1 — целый).

$R[s_1, s_2]$ — конечно порождённый $R[s_1]$ -модуль (аналогично: s_2 — целый над $R \Rightarrow s_2$ целый над $R[s_1]$).

$R[s_1, s_2]$ — конечно порождённый R -модуль: если $f \in R[s_1, s_2]$, то

$$f = \alpha_1 v_1 + \dots + \alpha_d v_d = \sum_{i=1}^d \sum_{j=1}^k \beta_{ij} m_j v_i$$

где v_i — образующие $R[s_1, s_2]$ как $R[s_1]$ -модуля, v_i — образующие $R[s_1]$ как R -модуля, $m_j v_i$ — образующие $R[s_1, s_2]$ как R -модуля.

Аналогично: $R[s_1, \dots, s_k]$ — конечно порождённый R -модуль. $\square$