Независимый Московский Университет

Алгебра – I

Первый курс, весенний семестр 1998/99 г.
Лекции 7–8

Отступление. Симметрические функции

Определение 1. Многочлен $f(x_1,\dots,x_n)\in\Bbbk[x_1,\dots,x_n]$ называется *симметрическим многочленом* (или *симметрической функцией*), если

$$f(x_{\sigma(1)},\dots,x_{\sigma(n)})=f(x_1,\dots,x_n)$$

для любой перестановки $\sigma\in S_n$.

Очевидно, что симметрические многочлены образуют подкольцо кольца $\Bbbk[x_1,\dots,x_n]$.

Определение 2. *Элементарным симметрическим многочленом* e_k (где $1\leqslant k\leqslant n$) называется сумма

$$\sum_{i_1<i_2<\dots<i_k} x_{i_1}x_{i_2}\dots x_{i_k}.$$

При $k=0$ полагаем $e_0=1$.

Основная теорема о симметрических функциях. *Всякий симметрический многочлен от $x_1,\dots,x_n$ единственным образом представляется в виде многочлена от элементарных симметрических многочленов $e_1,\dots,e_n$.*

Доказательство этой теоремы можно найти, к примеру, в книгах А. Н. Рудакова «Лекции по алгебре» (НМУ), Э. Б. Винберга «Начала алгебры» (НМУ), или А. И. Кострикина «Введение в алгебру».

Роль элементарных симметрических многочленов объясняется следующими *формулами Виета*.

Пусть $f(\lambda)=\sum a_k\lambda^k\in\Bbbk[\lambda]$ — многочлен степени n, а $\lambda_1,\dots,\lambda_n$ — его корни (каждый из которых написан столько раз, какова его кратность). Тогда для любого $k=0,1,\dots,n$

$$\frac{a_{n-k}}{a_n}=(-1)^k e_k(\lambda_1,\dots,\lambda_n).$$

Формулы Виета легко следуют из теоремы Безу.

Определение 3. *Полным симметрическим многочленом* h_k (где $k \in \mathbb{N}$) называется сумма

$$\sum_{i_1 \leqslant i_2 \leqslant \ldots \leqslant i_k} x_{i_1} x_{i_2} \ldots x_{i_k}.$$

При $k = 0$ полагаем $h_0 = 1$.

Определение 4. *Степенной суммой* s_k (где $k \in \mathbb{N}$) называется

$$\sum_{i=1}^{n} x_i^k.$$

При $k = 0$ степенная сумма не рассматривается.

По основной теореме о симметрических функциях, полные симметрические многочлены и степенные суммы можно выразить через элементарные симметрические многочлены. Оказывается, верно и обратное.

Утверждение 1. *1) Всякий симметрический многочлен от $x_1, \ldots, x_n$ представляется в виде многочлена от полных симметрических многочленов $h_1, \ldots, h_n$.*

2) Если $\operatorname{char} \Bbbk = 0$, то всякий симметрический многочлен от $x_1, \ldots, x_n$ представляется в виде многочлена от степенных сумм $s_1, \ldots, s_n$.

Доказательство. Согласно основной теореме о симметрических функциях, достаточно выразить элементарные симметрические многочлены. Для этого мы воспользуемся производящими функциями.

Напомню, что производящей функцией последовательности $(a_0, a_1, \ldots)$ элементов коммутативного кольца A называется формальный степенной ряд $\sum\limits_{k=0}^{\infty} a_k t^k \in A[[t]]$. Кроме обычных кольцевых операций, в кольце $A[[t]]$ есть операция дифференцирования по t:

$$\frac{d}{dt} \sum_{k=0}^{\infty} a_k t^k = \sum_{k=0}^{\infty} k a_k t^{k-1},$$

удовлетворяющая правилу Лейбница дифференцирования произведения: $(fg)' = f'g + fg'$. Отметим также, что формальный степенной ряд обратим тогда и только тогда, когда его свободный член обратим.

Легко видеть, что производящая функция для последовательности элементарных симметрических многочленов $(e_0, e_1, \ldots, e_n)$ имеет вид

$$e(t) = \prod_{i=1}^{n} (1 + x_i t),$$

а для последовательности полных симметрических многочленов $(h_0, h_1, \ldots)$ —

$$h(t) = \prod_{i=1}^{n} (1 - x_i t)^{-1}.$$

Отсюда получается равенство $e(t)h(-t) = 1$. Раскрывая скобки, получаем формулы

$$e_1 - h_1 = 0,$$

$$e_k + \sum_{l=1}^{k-1} (-1)^l e_{k-l} h_l + (-1)^k h_k = 0, \qquad (k > 1),$$

которые можно использовать в качестве рекуррентных формул для вычисления как (e_k) через (h_k), так и (h_k) через (e_k).

Производящей функцией для степенных сумм считается

$$s(t) = \sum_{k=1}^{\infty} s_k t^{k-1}.$$

Её связывает с $e(t)$ тоже почти очевидная формула

$$s(-t) = \frac{e'(t)}{e(t)}.$$

Упражнение 1. Докажите эту формулу.

Переписав эту формулу в виде $e(t)s(-t) = e'(t)$, получим соотношения (формулы Ньютона):

$$s_1 = e_1,$$

$$\sum_{l=1}^{k-1} (-1)^{l-1} e_{k-l} s_l + (-1)^{k-1} s_k = k e_k, \qquad (k > 1),$$

которые тоже можно использовать в качестве рекуррентных формул для вычисления как (e_k) через (s_k) (при $\operatorname{char} \Bbbk = 0$), так и (s_k) через (e_k) (в любом случае). $\square$

Единственность представления симметрической функции в виде многочлена от $h_1, \ldots, h_n$ (или от $s_1, \ldots, s_n$) тоже имеет место, но доказывать это мы не будем.

Основная теорема о конечных модулях над кольцами главных идеалов

Теорема 1. *Пусть* V *— конечный модуль над кольцом главных идеалов* R, *причем* $\operatorname{Ann}(V) = (p^m)$, *где* p *— некоторый простой элемент кольца* R. *Тогда* $V \cong R/(p^{k_1}) \oplus \dots \oplus R/(p^{k_r})$, *где* $k_1, \dots, k_r \in \mathbb{N}$, *причем набор показателей* k_i *однозначно определяется модулем* V.

Доказательство. Обозначим через $\mathcal{A}$ гомоморфизм $V \to V$, переводящий v в pv для любого $v \in V$. Положим $W_k = \mathcal{A}^{k-1}(V)$, $U = \operatorname{Ker}\mathcal{A}$ и $Q_k = W_k \cap U$. Тогда $W_{m+1} = 0$, но $W_m \neq 0$, и $U = Q_1 \supset Q_2 \supset \dots \supset Q_m = W_m \neq 0$. Отметим, что U имеет естественную структуру векторного пространства над полем $\Bbbk = R/(p)$. Выберем базис $(v_1^{(1)}, \dots, v_r^{(1)})$ пространства U следующим образом: вначале выберем произвольный базис пространства Q_m, затем дополним его до базиса Q_{m-1} и т. д. Для $s = 1, \dots, r$ обозначим через k_s такое натуральное число, что $v_s^{(1)} \in Q_{k_s} \setminus Q_{k_s+1}$ и выберем произвольный элемент $v_s \in V$, переходящий в $v_s^{(1)}$ под действием $\mathcal{A}^{k_s-1}$ (такой элемент существует по определению Q_{k_s}). Очевидно, что $\operatorname{Ann}(v_s) = (p^{k_s})$.

Докажем, что для любых $a_1, \dots, a_r \in R$ если $\sum a_s v_s = 0$, то $a_s v_s = 0$ для любого $s = 1, \dots, r$. Пусть это не так. Аннулятор любого элемента V порожден некоторой степенью p. Поэтому $\bigcap\limits_{s=1}^{r} \operatorname{Ann}(a_s v_s) = (p^k)$ для некоторого $k \in \mathbb{N}$. Тогда a_s делится на p^{k_s-k} для всех s таких, что $k_s > k$, причем a_s/p^{k_s-k} не кратно p хотя бы для одного значения s. Применяя $\mathcal{A}^{k-1}$ к $\sum a_s v_s = 0$, получаем нетривиальную линейную зависимость $\sum (a_s/p^{k_s-k}) v_s^{(1)} = 0$, что невозможно.

Отсюда следует, что существует инъективный гомоморфизм

$$\varphi : (R/(p^{k_1}) \oplus \dots \oplus R/(p^{k_r})) \to V,$$

переводящий $(\bar{a}_1, \dots, \bar{a}_r)$ в $\sum a_s v_s$. Докажем, что это изоморфизм.

Посчитаем длину R-модуля V. Заметим, что $Q_k = \operatorname{Ker}\mathcal{A}|_{W_k}$ и $\mathcal{A}(W_k) = W_{k+1}$. Отсюда $l(W_k) = l(W_{k+1}) + l(Q_k)$. С помощью индукции по $m - k$ отсюда следует, что $l(W_k) = \sum_{i=k}^{m} l(Q_i)$. Поскольку $V = W_1$, то $l(V) = \sum_{i=1}^{m} l(Q_i)$. Однако ровно такова длина модуля $R/(p^{k_1}) \oplus \dots \oplus R/(p^{k_r})$. Поэтому φ — изоморфизм.

Отметим теперь, что для $V = R/(p^{k_1}) \oplus \dots \oplus R/(p^{k_r})$ число слагаемых вида $R/(p^{k_s})$ с $k_s > k$ равно $l(p^k V / p^{k+1} V)$. Это доказывает, что набор k_s определен однозначно (с точностью до порядка). $\square$

Теорема 2. *Любой конечный модуль* V *над кольцом главных идеалов* R *изоморфен модулю вида* $\bigoplus\limits_{i=1}^{n} R/(p_i^{k_i})$, *где* p_i *— простые, причем набор идеалов* $(p_i^{k_i})$ *определен модулем* V *однозначно с точностью до перестановки.*

Доказательство. Доказательство проведем индукцией по $l(V)$. Для $l(V)=0$ доказывать нечего. Пусть $l(V)>0$ и $p\in R$ — простой элемент, делящий образующую идеала $\mathrm{Ann}(V)$. Тогда $pV\neq V$. Найдем минимальное натуральное число m такое, что $p^mV=p^{m+1}V$ (такое число найдется в силу конечности $l(V)$). Положим $W=p^mV$ и $U=\operatorname{Ker}\mathcal{A}^m$, где $\mathcal{A}:V\to V$ — гомоморфизм, переводящий v в pv для любого $v\in V$. Поскольку $W=p^{m+1}V=p(p^mV)=pW$, то $\mathcal{A}|_W$ — автоморфизм. Поэтому $U\cap W=0$. С другой стороны, $l(U)+l(W)=l(V)$, ибо $W\cong V/U$ по теореме о гомоморфизмах модулей. Поэтому $V=U\oplus W$. Аннулятор модуля U равен (p^m), следовательно, по предыдущей теореме U изоморфен модулю требуемого вида. $l(W)=l(V)-l(U)<l(V)$ и по предположению индукции модуль W тоже изоморфен модулю требуемого вида. То, что набор идеалов $(p_i^{k_i})$ определен однозначно с точностью до перестановки, доказывается так же, как в предыдущей теореме. $\square$

Пусть $a=p_1^{k_1}\cdot\dots\cdot p_n^{k_n}\in R$, где $p_1,\dots,p_n$ — различные простые элементы кольца R. Легко видеть, что $R/(a)\cong\bigoplus\limits_{i=1}^{n}R/(p_i^{k_i})$. Пользуясь этим, из доказанной нами теоремы легко вывести

Следствие 1. *Любой конечнопорожденный модуль кручения V над кольцом главных идеалов R изоморфен модулю вида $\bigoplus\limits_{i=1}^{r}R/(a_i)$, где $(a_1)\subseteq\dots\subseteq(a_r)\neq R$, причем набор идеалов (a_i) определен модулем V однозначно.*

Пример 1. Пусть $\Bbbk$ — любое поле, $f(x)=x^n+a_{n-1}x^{n-1}+\dots+a_0\in\Bbbk[x]$ и $V=\Bbbk[x]/(f)$ — циклический $\Bbbk[x]$-модуль. В базисе $v_1=\overline{1},v_2=\overline{x},\dots,v_n=\overline{x^{n-1}}$ матрица оператора, которым x действует в V, выглядит так:

$$\begin{pmatrix}0&0&0&\cdots&0&-a_0\\1&0&0&\cdots&0&-a_1\\0&1&0&\cdots&0&-a_2\\\vdots&\ddots&\ddots&\ddots&\vdots&\vdots\\0&0&0&\ddots&0&-a_{n-2}\\0&0&0&\cdots&1&-a_{n-1}\end{pmatrix}.$$

Такая матрица называется *циклическим блоком.*

Пусть матрица A — циклический блок, отвечающий многочлену $f(x)$. Тогда $f(A)=0$ (поскольку умножение на $f(x)$ аннулирует модуль $\Bbbk[x]/(f(x))$). Кроме того, так как векторы $v_1,v_2=Av_1,\dots,v_n=A^{n-1}v_1$ линейно независимы, то $f(x)$ — минимальный многочлен матрицы A. Разлагая $\det(\lambda E-A)$ по последнему столбцу, мы получаем, что характеристический многочлен циклического блока равен его минимальному многочлену.

Из следствия 1 мы получаем, что любой линейный оператор в конечномерном пространстве V над полем $\Bbbk$ в некотором базисе записывается блочно-диагональной матрицей A с циклическими блоками A_i на диагонали, причем минимальный многочлен A_i делится на минимальный многочлен A_{i+1}. Матрица A называется *фробениусовой нормальной формой* оператора.

Очевидно, что минимальный многочлен блока A_1 (который делится на минимальные многочлены всех остальных блоков) является минимальным многочленом матрицы A. С другой стороны, характеристический многочлен матрицы A равен произведению характеристических многочленов блоков A_i. Поэтому из существования фробениусовой нормальной формы следует, что для любого оператора характеристический многочлен делится на минимальный. Отсюда следует

Теорема 3 (Гамильтона-Кэли). *Характеристический многочлен оператора $\mathcal{A}$ аннулирует этот оператор.*

Свободные модули

Пусть R — коммутативное кольцо главных идеалов.

Определение 5. R-модуль V называется *свободным модулем ранга n*, если в у него есть базис из n элементов, то есть такие $v_1, \dots, v_n \in V$, что любой элемент $v \in V$ однозначно записывается в виде $v = \sum\limits_{i=1}^{n} c_i v_i$ с $c_i \in R$. Другими словами, R-модуль V является свободным модулем ранга n, если он изоморфен R-модулю R^n.

Отметим, что ранг свободного модуля определен однозначно. Действительно, пусть $p \in R$ — простой элемент, и $\Bbbk = R/(p)$. Тогда $R^n/pR^n = \Bbbk^n$, а размерность векторного пространства над полем $\Bbbk$ определена однозначно. (Для модулей над произвольным коммутативным кольцом рассуждение аналогичное, с заменой главного идеала, порожденного простым элементом, на любой максимальный идеал.)

Теорема 4. *Пусть R — кольцо главных идеалов, V — свободный R-модуль ранга n, и $W \subseteq V$ — подмодуль. Тогда модуль W тоже является свободным, и его ранг не превосходит n.*

Доказательство. Воспользуемся индукцией по n. При $n = 0$ доказывать нечего. Пусть $n > 0$. Обозначим через V_k подмодуль модуля V, порожденный элементами $v_1, \dots, v_k$. Очевидно, что V_k — свободный модуль ранга k.

Положим $I = \{a \in R \mid \text{в } W \text{ есть элемент вида } a_1 v_1 + \dots + a_{n-1} v_{n-1} + a v_n\}$. Тогда I — идеал. Пусть b — его образующая. Если $b = 0$, то $W = W \cap V_{n-1}$, и согласно предположению индукции W является свободным модулем ранга меньшего n. Предположим, что $b \neq 0$. Выберем в W элемент $w_n = b_1 v_1 + \cdots + b_{n-1} v_{n-1} + b v_n$. Пусть $w = a_1 v_1 + \cdots + a_{n-1} v_{n-1} + a v_n \in W$. Тогда $a = cb$ для некоторого $c \in R$ (определенного однозначно, ибо R — область целостности), и $w - c w_n \in W \cap V_{n-1}$. Поэтому $W = R w_n \oplus (W \cap V_{n-1})$. Как мы уже отмечали, $W \cap V_{n-1}$ является свободным модулем ранга меньшего n. Модуль $R w_n$ является свободным модулем ранга 1, поскольку $d w_n = d b_1 v_1 + \cdots + d b_{n-1} v_{n-1} + d b v_n \neq 0$ при $d \neq 0$. Следовательно, W — свободный модуль ранга не большего n. $\square$

Теорема 5. *Пусть кольцо R евклидово, V — свободный R-модуль ранга n, а $W \subseteq V$ — его подмодуль ранга k. Тогда существует такой базис $e_1, \dots, e_n$ модуля V, что $a_1 e_1, \dots, a_k e_k$ — базис модуля W, где $a_1, \dots, a_k \in R$, причем a_{i+1} делится на a_i при $i = 1, \dots, k-1$.*

Доказательство. Выберем произвольные базисы $(v_1, \dots, v_n)$ модуля V и $(w_1, \dots, w_k)$ модуля W. Мы имеем $w_i = \sum_{j=1}^{n} c_{ij} v_j$ для некоторой $k \times n$ матрицы $C = (c_{ij})$ с коэффициентами из R. Элементарным преобразованиям строк матрицы C отвечают замены базиса в W, а элементарным преобразованиям столбцов матрицы C отвечают замены базиса в V. Нам надо доказать, что с помощью таких операций матрицу C можно привести к матрице, у которой на диагонали стоят элементы $a_1, \dots, a_k$, а на остальных местах — нули, причем a_{i+1} делится на a_i при $i = 1, \dots, k-1$.

Воспользуемся евклидовостью кольца R, то есть тем, что каждому ненулевому элементу $a \in R$ поставлено в соответствие натуральное число $\delta(a)$, которое мы будем называть абсолютным значением, причем $\delta(ab) \geqslant \delta(a)$ и возможно деление с остатком. Прежде всего применим элементарные преобразования столбцов и строк так, чтобы наименьшее абсолютное значение ненулевого элемента матрицы стало минимально возможным. После этого переставим столбцы и строки так, чтобы элементом с наименьшим собственным значением оказался c_{11}. Вычтем первую строку с подходящими коэффициентами из остальных строк так, чтобы первые элементы каждой строки стали минимальными (деление с остатком), то есть равными нулю (ибо, по предположению, мы не можем получить матричный элемент с абсолютным значением меньшим чем $\delta(c_{11})$). Аналогичным образом обратим в нуль первые элементы всех столбцов. Теперь заметим, что все матричные элементы полученной матрицы должны делиться на c_{11}. Действительно, если c_{ij} не делится на c_{11}, то $c_{ij} = d c_{11} + r$ для некоторых $d, r \in R$, причем $\delta(r) < \delta(c_{11})$. Прибавив первую строку к i-той, а затем вычтя из j-го столбца первый, умноженный на d, получим матрицу с матричным элементом r. Это противоречит предположению о том, что $\delta(c_{11})$ уже нельзя уменьшить. Итак, мы получили матрицу вида

$$\begin{pmatrix} c_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & C' & \\ 0 & & & \end{pmatrix},$$

причем все матричые элементы матрицы C' делятся на c_{11}. Применим теперь описанную выше процедуру к матрице C'. При этом она приведется к виду

$$\begin{pmatrix} c_{22} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & C'' & \\ 0 & & & \end{pmatrix},$$

где c_{22} делится на c_{11} и все матричные элементы C'' делятся на c_{22}. Продолжая этот процесс, получаем матрицу требуемого вида. $\square$

Заметим, что каждый конечнопорожденный модуль является образом свободного модуля конечного ранга под действием гомоморфизма. Действительно, если $v_1, \ldots, v_n$ порождают модуль V, то гомоморфизм $\varphi : R^n \to V$, переводящий $(a_1, \ldots, a_n)$ в $a_1 v_1 + \cdots + a_n v_n$, является сюръективным. Положим $W = \operatorname{Ker} \varphi$. Если R — евклидово, то мы можем воспользоваться последней теоремой, чтобы получить другое доказательство следствия 1.

Кроме того, легко доказать (даже для произвольных колец главных идеалов), что любой конечнопорожденный модуль является прямой суммой своего подмодуля кручения и некоторого свободного модуля. Это позволяет обобщить теорему 2 на все конечнопорожденные модули.

Приложение. Еще одно доказательство теоремы Гамильтона-Кэли

Пусть B — матрица размера $n \times n$ над произвольным коммутативным кольцом R. Мы можем рассматривать B как матрицу гомоморфизма R-модуля $V = R^n$ в себя. Пусть $W \subseteq V$ — такой подмодуль, что $B(V) \subseteq W$. Тогда $(\det B)V \subseteq W$. Действительно, пусть $\hat{B}$ — присоединенная матрица, то есть такая, у которой на месте ij стоит алгебраическое дополнение B_{ji}. Тогда $B\hat{B} = (\det B)E$, так что $(\det B)V = B\hat{B}(V) = B(\hat{B}(V)) \subseteq W$.

Пусть A — квадратная $n \times n$ матрица над полем $\Bbbk$. Рассмотрим матрицу $B = xE - A$ над кольцом $R = \Bbbk[x]$. Положим $V = R^n$, $W = B(V)$. Фактормодуль V/W естественно изоморфен $\Bbbk^n$, в котором x действует линейным оператором с матрицей A. По доказанному выше, умножение на характеристический многочлен $p(x) = \det(xE - A)$ переводит V в W, то есть $p(x)$ действует в V/W нулем. Тем самым $p(A) = 0$.