Лекция 8
Алгебраические функции

▹Лексикографическое упорядочение мономов ▹Формулы Виета ▹Разложение на множители результанта и дискриминанта ▹Базисы в модуле симметрических многочленов ▹Основная теорема о симметрических функциях ▹Рациональные функции ▹Разложение на простейшие дроби ▹Поле частных ▹Ряды Лорана и дробно-степенные ряды ▹Разложение неявной алгебраической функции в формальный дробно-степенной ряд

Функции, как правило, задаются алгебраическими формулами. При работе с такими функциями возникают два вопроса: первый – как определить значение функции в точке, или более общо, как придать смысл высказыванию: "такая-то алгебраическая формула определяет нам функцию"; второй – как с такими формулами производить вычисления, то есть устанавливать для таких функций те или иные тождества. Первое поле деятельности традиционно относится к анализу, а второе - к алгебре. Ближайшие две лекции мы будем заниматься именно этой второй задачей — обсудим как производить вычисления над функциями (образующими, как правило, некую стандартную алгебраическую структуру), и установим ряд классических соотношений.

§1. Многочлены от многоих переменных

В этом пункте мы применим векторную машинерию к тому, чтобы систематизировать наши представления о $K[x_1, x_2, \dots, x_n]$ как о K-модуле. Кольцо K теперь будет произвольным коммутативным кольцом с единицей.

1.1. Упорядочение мономов. Базис в K-модуле $K[x_1, x_2, \dots, x_n]$ составляют (по определению многочленов) всевозможные мономы $x_1^{d_1}, x_2^{d_2}, \dots, x_n^{d_n}$. Целое неотрицательное число $|d| \overset{\text{def}}{=} \sum\limits_i d_i$ называется *степенью* монома, а сам набор $d = (d_1, d_2, \dots, d_n)$ – *мультистепенью*. Мы часто будем сокращать запись $x_1^{d_1}, x_2^{d_2}, \dots, x_n^{d_n}$ до x^d. При этом удобно представлять себе $d = (d_1, d_2, \dots, d_n)$ как вектор, лежащий в первом координатном октанте решётки $\mathbb{Z}^n$.

Выше мы привыкли иметь дело с базисами, векторы в которых линейно упорядочены: $e_1, e_2, \dots$. Линейная упорядоченность базисных векторов необходима, к например, для того чтобы записывать гомоморфизмы матрицами. На множестве наборов $d = (d_1, d_2, \dots, d_n)$ имеется стандартный линейный порядок, который называется *лексикографическим*, ибо основан на том же принципе, что и расположение слов в словаре: мультистепень $a = (a_1, a_2, \dots, a_n)$ называется *лексикографически большей*, чем мультистепень $b = (b_1, b_2, \dots, b_n)$, если для некоторого i имеем $a_\nu = b_\nu$ при $\nu < i$, но $a_i > b_i$. В этом случае мы будем писать $a > b$.

Задача 8.1. Убедитесь, что мы действительно определили на множестве мультистепеней отношение полного линейного порядка (т. е. проверьте, что $\forall a, b$ имеются в точности 3 взаимо исключающие возможности: $a < b$, $a = b$, $b < a$, что из неравенств $a > b$ и $b > c$ следует неравенство $a > c$ и что в каждом непустом множестве мультииндексов есть наименьший элемент).

1.1.1. Пример: однородные многочлены степени d — это многочлены, каждый моном которых имеет степень d. Они составляют свободный подмодуль в $K[x_1, x_2, \ldots, x_n]$ ранга $\binom{d+n-1}{n}$ (почему?). Лекикографически старшим мономом в этом модуле является x_1^d, а лексикографически младшим - моном x_n^d.

Задача 8.2. Докажите, что $f \in K[x_1, x_2, \ldots, x_n]$ тогда и только тогда однороден степени d, когда в кольце $K[t, x_1, x_2, \ldots, x_n]$ выполнено равенство $f(tx_1, tx_2, \ldots, tx_n) = tf(x_1, x_2, \ldots, x_n)$.

Задача 8.3. (Теорема Эйлера об однородных функциях.) Докажите, что $f \in K[x_1, x_2, \ldots, x_n]$ тогда и только тогда однороден степени d, когда в кольце $K[x_1, x_2, \ldots, x_n]$ выполнено равенство $\sum\limits_{i=1}^{n} \dfrac{\partial f}{\partial x_i} = d \cdot f$ (через $\dfrac{\partial f}{\partial x_i}$ обозначается производный многочлен от $f(x_1, x_2, \ldots, x_n)$, рассматриваемого, как многочлен от x_i с коэффициентами из кольца многочленов от остальных переменных).

1.2. Сравнение соответственных мономов. Наличие линейного порядка на мономах позволяет распространить на кольцо $K[x_1, x_2, \ldots, x_n]$ стандартные свойства умножения в $K[x]$.

Задача 8.4. Убедитесь, что старший и младший мономы в произведении равны, соответственно, произведениям старших и младших мономов сомножителей.

В частности, отсюда следует, что в $K[x_1, x_2, \ldots, x_n]$ не будет делителей нуля, если их не было в K, и что обратимыми элементами в $K[x_1, x_2, \ldots, x_n]$ являются обратимые константы и только они.

При доказательстве различных тождеств часто очень эффективным оказывается *сравнение старших членов*. Стандартная схема такова. Допустим, что нам надо разложить многочлен f на множители, и мы из каких-то соображений знаем, что f делится на многочлены $g_1, g_2, \ldots, g_k$. Тогда, если старший моном у произведения $g_1 g_2 \cdots g_k$ имеет ту же мультистепень, что и старший моном в f, то $f = c \cdot g_1 g_2 \cdots g_k$, где $c \in K$ – константа, и для нахождения точного значения c, опять же, достаточно сравнить лишь коэффициенты при старших мономах.

1.2.1. Пример: определитель ван дер Монда

$$\det \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ x_1 & x_2 & x_3 & \ldots & x_n \\ x_1^2 & x_2^2 & x_3^2 & \ldots & x_n^2 \\ \vdots & \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \ldots & x_n^{n-1} \end{pmatrix} = \prod_{i>j} (x_i - x_j) \quad .$$

Действительно, обе части являются элементами $\mathbb{Z}[\, x_1, x_2, \ldots, x_n \,]$, причём левый многочлен делится на правый, ибо он делится на каждый из попарно взаимно простых линейных двучленов $(x_i - x_j)$ (чтобы убедиться в этом надо отнять из i-того столбца j-тый и вынести $(x_i - x_j)$ из каждогой разности $x_i^k - x_j^k$). Остаётся заметить, что старшие мономы слева и справа одинаковы – это $(-1)^{\frac{n(n-1)}{2}} x_1^{n-1} x_2^{n-2} x_3^{n-3} \cdots x_{n-1}$.

Задача 8.5. Убедитесь в этом!

1.3. Формулы Виета. Пусть $\{x_1, x_2, \ldots, x_n\}$ – корни многочлена $f(t) = a_0t^n + a_1t^{n-1} + \cdots + a_{n-1}t + a_n \in K[t]$, где K – произвольное коммутативное кольцо. Тогда, как мы знаем, $f(t)$ делится на произведение $(t - x_1)(t - x_2)\cdots(t - x_n)$, и сравнивая старшие степени t, мы получаем разложение:

$$a_0t^n + a_1t^{n-1} + \cdots + a_{n-1}t + a_n = a_0(t - x_1)(t - x_2)\cdots(t - x_n) ,$$

которое позволяет выразить коэффициенты $a_1, a_2, \ldots, a_n$ через a_0 и корни $x_1, x_2, \ldots, x_n$. Действительно, сравнивая коэффициент при t^{n-k}, мы получаем

1.3.1. Предложение. (Теорема Виета.)

$$a_k = (-1)^k a_0 e_k(x_1, x_2, \ldots, x_n) ,$$

где $e_k(x_1, x_2, \ldots, x_n) \stackrel{\text{def}}{=} \sum\limits_{1\le\nu_1<\nu_2<\cdots<\nu_k\le n} x_{\nu_1}x_{\nu_2}\cdots x_{\nu_n}$ *есть сумма всех возможных произведений из k попарно разных переменных ($k = 1, 2, \ldots, n$).*

□

Многочлены $e_k(x_1, x_2, \ldots, x_n)$ называются *элементарными симметрическими многочленами.*

Задача 8.6. Пусть $s_i = x_i^{-1}$, $i = 1, 2, \ldots, n$ — величины, обратные к корням. Убедитесь, что имеется разложение

$$a_0t^n + a_1t^{n-1} + \cdots + a_{n-1}t + a_n = a_n(1 - s_1t)(1 - s_2t)\cdots(1 - s_nt)$$

и докажите формулы $a_k = (-1)^{n-k}a_ne_{n-k}(s_1, s_2, \ldots, s_n)$.

1.4. Разложение результанта и дискриминанта. Пусть K – произвольное коммутативное кольцо. Рассмотрим кольцо многочленов $\mathcal{K} = K[\,x_1, x_2, \ldots, x_n\,,\ y_1, y_2, \ldots, y_m\,]$ и будем воспринимать переменные $x_1, x_2, \ldots, x_n$ как формальные корни многочлена

$$f(t) = a_0\prod_{\nu=1}^{n}(t - x_\nu) = a_0t^n + a_1t^{n-1} + \cdots + a_{n-1}t + a_n \in \mathcal{K}[t] ,$$

а переменные $y_1, y_2, \ldots, y_m$ — как формальные корни многочлена

$$g(t) = b_0\prod_{\mu=1}^{n}(t - y_\mu) = b_0m^t + b_1m^{t-1} + \cdots + b_{t-1}m + b_t \in \mathcal{K}[t] .$$

Мы собираемся разложить на множители результант $R(f, g)$ как элемент кольца

$$\mathcal{K}' = K[\,a_0, a_1, \ldots, a_n\,,\ b_0, b_1, \ldots, b_m\,] .$$

Для этого заметим, что при подстановке y_j вместо x_i, многочлены f и g приобретают общий корень, а стало быть, результант в этом случае обратится в ноль.

Задача 8.7. Убедитесь, что если многочлен от x, y (с коэффициентами в любом коммутативном кольце) обращается в ноль при замене всех входящих в него x'ов на y, то он делится нацело на $x - y$.

Указание. Это вполне аналогично Сл.2.2.1 из лекции 3.

Поскольку все разности $x_i - y_j$ попарно взаимно просты, и все коэффициенты f делятся на a_0, а все коэффициенты g делятся на b_0, результант $R(f,g)$ делится в кольце

$$K[\,x_1, x_2, \dots, x_n\,,\ y_1, y_2, \dots, y_m\,,\ a_0,\ b_0] \supset \mathcal{K}'$$

на произведение

$$P = a_0^m b_0^n \prod_{\substack{1\le\nu\le n\\ 1\le\mu\le m}} (x_\nu - y_\mu) = a_0^m \prod_{\nu=1}^{n} g(x_\nu) = (-1)^{mn} b_0^n \prod_{\mu=1}^{m} f(y_\mu)\,.$$

Из последних двух перезаписей видно, что P как элемент $\mathcal{K}'$ является однородным степени n по переменным b_i, и однородным степени m по переменным a_j.

Задача 8.8. Убедитесь, что результант $R(F,G)$ любых двух многочленов F и G однороден степени $\deg G$ по коэффициентам F и однороден степени $\deg F$ по коэффициентам G.

Таким образом, $R(f,g) = \mathrm{const}\cdot P$. Сравнение коэффициена при $a_0^m b_m^n$ в $R(f,g)$ и P показывает, что константа равна единице.

Задача 8.9. Чему точно равны сравниваемые коэффициенты?

Итак, мы доказали

1.4.1. Предложение. *Результант $R(f,g)$ пары многочленов f и g (над произвольным коммутативным кольцом), имеющих корни $x_1, x_2, \dots, x_n$ и $y_1, y_2, \dots, y_m$ и старшие коэффициенты a_0 и b_0 допускает разложения*

$$R(f,g) = a_0^m b_0^n \prod_{\substack{1\le\nu\le n\\ 1\le\mu\le m}} (x_\nu - y_\mu) = a_0^m \prod_{\nu=1}^{n} g(x_\nu) = (-1)^{mn} b_0^n \prod_{\mu=1}^{m} f(y_\mu)\,.$$

□

1.4.2. Следствие. *Дискриминант $D(f)$ многочлена f (над произвольным коммутативным кольцом), имеющего корни $x_1, x_2, \dots, x_n$ и старший коэффициент a_0 допускает разложение*

$$D(f) = a_0^{2n-2} \prod_{i>j} (x_i - x_j)^2 = a_0^{2n-2} \det{}^2 \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ x_1 & x_2 & x_3 & \dots & x_n \\ x_1^2 & x_2^2 & x_3^2 & \dots & x_n^2 \\ \vdots & \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \dots & x_n^{n-1} \end{pmatrix}.$$

Доказательство. По определению, $D(f) = (-1)^{\frac{n(n-1)}{2}} R(f,f')$. Но выше мы видели, что $R(f,f') = a_0^{n-1}\prod\limits_i f'(x_i)$. Но по формуле для дифференцирования произведения мы имеем

$$f'(x_i) = \left.\frac{d}{dt}\right|_{t=x_i} a_0 \prod_{\nu} (t - x_\nu) = a_0 \prod_{\nu\ne i} (x_i - x_\nu)\,,$$

откуда после перемножения и получается нужное равенство.

□

Задача 8.10. Докажите, что дискриминант и результант являются неприводимыми многочленами от коэффициентов исходных многочленов.

Задача 8.11. Докажите, что дискриминант $D(a_0t^n + a_1t^{n-1} + \dots + a_{n-1}t + a_n)$ как функция от коэффициентов a_i удовлетворяет дифференциальному уравнению

$$na_0 + (n-1)a_1\frac{\partial D}{\partial a_2} + (n-2)a_2\frac{\partial D}{\partial a_3} + \dots + \frac{\partial D}{\partial a_n}\,.$$

Указание: Проверьте сначала, что дискриминант инвариантен относительно сдвигов переменной, т. е. $D\Big(f(t)\Big) = D\Big(f(t+a)\Big)\ \ \forall\, a \in K$.

§2. Симметрические многочлены

2.1. Определение. *Многочлен $f(x_1, x_2, \dots, x_n)$ называется симметрическим, если он не изменяется при любой перенумерации переменных, т. е. если*

$$f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) = f(x_1, x_2, \dots, x_n) \qquad \forall\, \sigma \in \mathfrak{S}_n\ .$$

Ясно, что симметрические многочлены из $K[x_1, x_2, \dots, x_n]$ образуют K-модуль (над произвольным коммутативным кольцом K).

Из теоремы Виета следуетет, что коэффициенты и дискриминант приведенного многочлена $t^n + a_1t^{n-1} + \dots + a_{n-1}t + a_n \in k[t]$ являются симметрическими многочленами от его корней. Оказывается, имеет место следующее

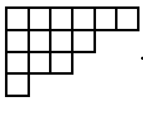
2.1.1. Предложение. *Всякий симметрический многочлен от корней приведенного многочлена из $k[t]$ может быть выражен в виде многочлена от коэффициентов (а стало быть, его значения можно найти не решая уравнения).*

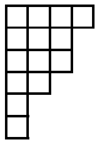
Мы докажем сейчас несколько более сильный результат: проверим, что многочлены вида

$$e_1^{d_1}e_2^{d_2}\cdots e_n^{d_n}\ ,$$

где $e_k(x_1, x_2, \dots, x_n) = \sum\limits_{1 \le \nu_1 < \nu_2 < \dots < \nu_k \le n} x_{\nu_1}x_{\nu_2}\cdots x_{\nu_n}$ суть элементарные симметрические многочлены, составляют *базис* модуля симметрических многочленов. Обозначим через $Sym^d = Sym^d(x_1, x_2, \dots, x_n)$ подмодуль, состоящий из однородных симметрических многочленов степени d и нулевого многочлена. Поскольку элементарный симметрический многочлен e_k однороден степени k, нам достаточно будет проверить, что многочлены вида $e_1^{d_1}e_2^{d_2}\cdots e_n^{d_n}$ с $\sum\limits_k kd_k = m$ образуют базис в Sym^m при каждом m. В процессе проверки нам понадобится одно очень полезное обозначение.

2.2. Разбиения и диаграммы Юнга. Упорядоченный набор монотонно невозрастающих неотрицательных целых чисел $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k)$, $\lambda_1 \ge \lambda_2 \ge \dots \ge \lambda_k \ge 0$, с суммой $\sum \lambda_i = n$ называется *разбиением числа* n. Число n называется *весом* разбиения λ и обозначается также через $|\lambda|$. Число k называется *длиной* разбиения и обозначается $l(\lambda)$.

Визуализируется разбиение при помощи картинки, которая называется *диаграммой Юнга* и сосотоит из расположенных друг под другом и выровненных по левому краю клетчатых полосок длины $\lambda_1, \lambda_2, \dots, \lambda_k$ (удобно рисовать на клетчатой бумаге). Например, разбиение $\lambda = (6431)$ изображается диаграммой . Разбиение, отвечающее *транспонирован-*

ной (т. е. симметричной относительно главной диагонали) диаграмме  называется *сопряжённым* к исходжному и обозначается λ' (в нашем случае $\lambda' = (4,3,3,2,1,1)$).

Задача 8.12. Убедитесь, что $\lambda'_i =$ (количество строк длины $\le i$ в λ).

2.3. Симметрические многочлены e_λ. Соответсвие

$$\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k) \longmapsto e_\lambda \overset{\text{def}}{=} e_{\lambda_1} e_{\lambda_2} \cdots e_{\lambda_k}$$

устанавливает биекцию между всевозможными многочленами вида $e_1^{d_1} e_2^{d_2} \cdots e_n^{d_n}$ лежащими в Sym^d и всевозможными разбиениями λ веса d, такими что $l(\lambda') = n$ (обратное отображение сопоставляет каждому многочлену вида $e_1^{d_1} e_2^{d_2} \cdots e_n^{d_n}$ разбиение

$$\lambda = (\underbrace{n, n, \dots, n}_{d_n}, \underbrace{(n-1), (n-1), \dots, (n-1)}_{d_{n-1}}, \dots \underbrace{1, 1, \dots, 1}_{d_1}) ,$$

в котором количество строк длины i равно показателю при e_i).

2.3.1. Лемма. *Лексикографически старший моном многочлена $e_\lambda = e_{\lambda_1} e_{\lambda_2} \cdots e_{\lambda_k}$ равен $x_1^{\lambda'_1} x_2^{\lambda'_2} \cdots x_n^{\lambda'_n}$, где $\lambda' = (\lambda'_1, \lambda'_2, \dots, \lambda'_n)$ – сопряжённое к λ разбиение.*

Доказательство. Поскольку старший моном в e_i есть $x_1 x_2 \cdots x_i$, степень, в которой переменная x_m войдет в старший моном произведения $e_{\lambda_1} e_{\lambda_2} \cdots e_{\lambda_k}$ равна количеству строк в λ, длина которых не меньше, чем m.
□

2.4. Симметрические многочлены f_λ. Для прозвольного разбиения $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_n)$ обозначим через $f_\lambda \in Sym^{|\lambda|}$ сумму всех попарно различных мономов, которые можно получить из монома $x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n}$ всевозможными перенумерациями переменных. Симметрические многочлены f_λ называются *мономиальными* симметрическими многочленами.

2.4.1. Лемма. *Sym^d является свободным K-модулем конечного ранга, и всевозможные многочлены f_λ с $l(\lambda) = n$, $|\lambda| = d$ составляют базис в Sym^d.*

Доказательство. Всякий полином $g \in Sym^d$ вместе с каждым мономом содержит и все мономы, получающиеся из него перенумерациями переменных, причём все эти мономы входят в g с одним итем же коэффициентом, и лексикографически старшим из них будет единственный моном $c_\lambda \cdot x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n}$, показатели которого невозрастают: $\lambda_1 \ge \lambda_2 \ge \dots \ge \lambda_n$. Стало быть, сумма всех этих мономов есть $c_\lambda \cdot f_\lambda$, где $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_n)$, $c_\lambda \in K$. Это показыает, что g распадается и притом единственным образом в линейную комбинацию многочленов f_λ с коэффициентами из K.
□

2.5. Матрица перехода от e_λ к f_λ. Введм лексикографический порядок на множестве всех разбиений $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_n)$ веса d и длины n. Тогда согласно Лм.2.3.1 разложение многочлена e_λ по базису f_λ имеет вид

$$e_\lambda = f_{\lambda'} + \text{ члены младших степеней },$$

где λ' — разбиение, двойственное к λ. Таким образом, если ввести на множестве всех разбиений веса d, удовлетворяющих условию $l(\lambda') = n$, линейное упорядочение полагая $\lambda < \mu$ если λ' лексикографически меньше μ', то мы получим

2.5.1. Следствие. *Матрица, по столбцам которой стоят координаты многочленов $e_\lambda \in Sym^n$ в базисе из мономиальных симметрических многочленов, является квадратной верхнетреугольной матрицей с единицами по главной диагонали.*

□

Но всякая матрица $H = (h_{ij} \in Mat_N(K)$, у которой $h_ij = 0$ при $i > j$ и $h_{ii} = 1$ $\forall i$ обратима над любым кольцом K.

Задача 8.13. Докажите это и получите (хотя бы при малых N) общую формулу для обратной матрицы.

Ответ: обратная матрица $H^{-1} = (g_{ij})$ имеет

$$g_{ij} = \begin{cases} 0 \quad \text{при} \quad i > j \\ 1 \quad \text{при} \quad i = j \\ -h_{ij} + \sum\limits_{i<\nu_1<j} h_{i\nu_1}h_{\nu_1 j} - \sum\limits_{i<\nu_1<\nu_2<j} h_{i\nu_1}h_{\nu_1\nu_2}h_{\nu_1 j} + \sum\limits_{i<\nu_1<\nu_2<\nu_3<j} \cdots \qquad \text{при} \quad i < j \end{cases}.$$

Как мы знаем, обратимость матрицы перехода равносильно тому, что e_λ также составляет базис в Sym^d.

2.5.2. Следствие. *Многочлены $e_\lambda = e_{\lambda_1}e_{\lambda_2}\cdots e_{\lambda_k}$, где λ пробегает разбиения веса d, у которых $l(\lambda') = n$, или (что то же самое) многочлены вида $e_1^{d_1}e_2^{d_2}\cdots e_n^{d_n}$ с $\sum\limits_k kd_k = d$ составляют базис модуля $\sum^d$ однородных симметрических многочленов степени d над произвольным коммутативным кольцом K.*

□

Переформулировкой этого следствия является

2.6. Теорема. (Основная теорема о симметрических функциях.) *Гомоморфизм*

$$K[t_1, t_2, \ldots, t_n] \to K[x_1, x_2, \ldots, x_n]\ ,$$

переводящий многочлен $p(t_1, t_2, \ldots, t_n)$ в многочлен $p(e_1(x), e_2(x), \ldots, e_n(x))$ отождествляет $K[xt1, t_2, \ldots, t_n]$ с подкольцом симметрических многочленов в $K[x_1, x_2, \ldots, x_n]$, т. е. всякий симметрический многочлен может быть представлен в виде многочлена от элементарных симметрических многочленов

$$e_i(x) \in K[x_1, x_2, \ldots, x_n]\ ,$$

и такое представление единственно.

□

2.7. Практическое отыскание представления $g(x) = p(e)$ данного симметрического многочлена $g \in Sym^d$ в виде многочлена от элементарных симметрических многочленов осуществляется обычно так. В $g(x)$ отыскивается лексикографически старший моном

$$\alpha \cdot x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_n^{\lambda_n}$$

Его показатели автоматически невозрастают: $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$, и многочлен $g(x) - \alpha \cdot e_{\lambda'}(x)$, где λ' – разбиение, двойственное к $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n)$, имеет лексикографически меньший старший моном, чем $g(x)$. Далее процесс продолжается по индукции.

Задача 8.14. Пусть x_+ и x_- – корни уравнения $at^2 + bt + c = 0$. Не прибегая к определителям, выразите $D = a(x_+ - x_-)^2$ через a, b, и c и выведите из этого всю школьную теорию квадратных уравнений.

Задача 8.15. Пусть x_1, x_2, x_3 – корни уравнения $x^3 + px + q = 0$. Не прибегая к определителям, выразите $D = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$ через p и q.

§3. Рациональные функции

3.1. Терминология. Класс эквивалентных дробей P/Q, где P, $Q \in k[x_1, x_2, \dots, x_n]$, $Q \neq 0$ и P/Q и F/G считаются эквивалентными, если $P(x)G(x) = F(x)Q(x)$ в $k[x_1, x_2, \dots, x_n]$, называется *рациональной функцией* от n переменных над полем k. Про эквивалентные дроби P/Q и F/G говорят, что они задают одну и туже рациональную функцию. Множество рациональных функций обозначается $k(x_1, x_2, \dots, x_n)$ (скобки круглые). Определим в $k(x_1, x_2, \dots, x_n)$ сложение и умножение формулами

$$\begin{gathered}\frac{P_1}{Q_1} + \frac{P_2}{Q_2} \stackrel{\text{def}}{=} \frac{P_1 Q_2 + P_2 Q_1}{Q_1 Q_2} \\ \frac{P_1}{Q_1} \cdot \frac{P_2}{Q_2} \stackrel{\text{def}}{=} \frac{P_1 P_2}{Q_1 Q_2}\,.\end{gathered} \tag{8-1}$$

Задача 8.16. Проверьте, что эти определения корректны, (т. е. не зависят от выбора представителя в классе эквивалентных дробей).

Задача 8.17. Убедитесь (прямой проверкой всех аксиом надлежащими явными вычислениями), что $k(x_1, x_2, \dots, x_n)$ является полем.

Запись рациональной функции дробью P/Q называется *несократимой*, если полиномы P и Q не имеют нетривиальных общих делителей. Дробь P/Q называется *правильной*, если $\deg P < \deg Q$.

Задача 8.18. Убедитесь, что свойство дроби быть правильной сохраняется при переходе к эквивалентной дроби.

3.2. Разложение рациональных функций от одной переменной. При вычислениях с рациональными функциями от одной переменной над полем часто бывает полезной следующая

3.2.1. Лемма. *Пусть k – поле, и путь знаменатель дроби $P(t)/Q(t) \in k(t)$ разложен в произведение попарно взаимно простых многочленов:*

$$Q(t) = q_1(t) q_2(t) \dots q_m(t)\,.$$

Тогда существует разложение

$$\frac{P(t)}{Q(t)} = h(t) + \frac{p_1(t)}{q_1(t)} + \frac{p_2(t)}{q_2(t)} + \dots + \frac{p_m(t)}{q_m(t)}\,, \tag{8-2}$$

в котором $\deg h = \deg P - \deg Q$, $\deg p_i < \deg q_i$ и набор многочленов h, $p_1, p_2, \dots, p_m \in k[t]$ однозначно определяется этими условиями по P и Q.

Доказательство. Пусть требуемое равенство выполнено. Домножая обе его части на Q, получим в $k[t]$ равенство:

$$P = hQ + p_1 Q_1 + p_2 Q_2 + \dots + p_m Q_m\,, \tag{8-3}$$

где через Q_i обозначено произведение всех многочленов q_ν кроме i-того (в частности, Q_i взаимно прост с q_i и делится на все $q\nu$ с $\nu \neq i$). Из условия леммы вытекает неравенство $\deg(\sum p_\nu Q_\nu) < \deg Q$, показывающее, что h и $r \stackrel{\text{def}}{=} \sum p_\nu Q_\nu$ однозначно определяются как неполное частное и остаток от деления P на Q. Поскольку Q_i обратим в кольце $k[t]/(q_i)$, каждый из p_i однозначно определяется как единственный многочлен степени $< \deg q_i$, представляющий класс вычета $[r][Q_i]^{-1} = [P][Q_i]^{-1}$ в кольце $k[t]/(q_i)$ вычетов по $\mod q_i$.

Это рассуждение показывает не только единственность, но и существование. Действительно, деля P на Q с остатком, можем написать, что $P/Q = h + r/Q$, где $\deg P < \deg Q$. Далее, подбирая $p_1 \in k[t]$ с $\deg p_1 < \deg q_1$, представляющий в $k[t]/(q_1)$ класс $[P][Q_1]^{-1}$, можем написать, что $r = p_1Q_1 + q_1r_1$, с некоторым $r_1 \in k[t]$, имеющим $\deg r_1 < \deg Q_1$ (ибо $\deg r < \deg Q$). Отсюда $r/Q = p_1/q_1 + r_1/Q_1$, где знаменатель Q_1 уже не содержит q_1, но по-прежнему $\deg r_1 < \deg Q_1$, так что процедуру можно повторить с r_1/Q_1 и так далее.
□

3.2.2. Практическое отыскание разложения (8-2) удобно производить методом неопределенных коэффициентов: поскольку мы знаем оценки сверху на степени h и p_i, мы можем записать эти многочлены с неопределенными коэффициентами, и воспринимать соотношение (8-3) как систему линейных уравнений на эти коэффициенты. При этом извлекать из (8-3) уравнения можно двумя способами: либо приравнивать коэффициенты при одинаковых степенях t в левой и правой части, либо подставлятьть в левую и правую часть конкретные значения $t \in k$ (в качестве таковых особенно удобны корни многочленов q_i, ибо они аннулируют все Q_ν кроме i-того).

3.2.3. Пример: Найдём 1996-ю производную от $f(x) = x^3/(1+x^2)$, для чего воспользуемся разложением

$$\frac{x^3}{x^2+1} = x + \frac{\alpha}{x+i} + \frac{\beta}{x-i}$$

с подходящими $\alpha, \beta \in \mathbb{C}$. Чтобы их найти, подставим в равенство

$$x^3 = x(x^2+1) + \alpha(x-i) + \beta(x+i)$$

значения $x = i$ и $x = -i$. Получим $2i\beta = -i$ и $-2i\alpha = i$, т. е. $\alpha = \beta = -1/2$. Для 1996-й производной получаем выражение

$$-1995!\left((x+i)^{-1996} + (x-i)^{-1996}\right) = -1995! \cdot 2 \cdot \frac{x^{1996} + \binom{1996}{2}x^{1994} + \binom{1996}{4}x^{1992} + \cdots + 1}{(x^2+1)^{1996}}\,.$$

Задача 8.19. Докажите, что правильная дробь вида P/Q^d, однозначно записывается в виде

$$\frac{P}{Q^d} = \frac{P_1}{Q} + \frac{P_2}{Q^2} + \cdots + \frac{P_d}{Q^d}\,,$$

где $\deg P_i < \deg Q \qquad \forall i$.

Указание. Это не что иное как введение на кольце многочленов Q-ической позиционной системы счисления, что вполне аналогично хорошо известной всем программистам деятельности с натуральными числами (см. задачу ниже).

Задача 8.20. Докажите, что всякое натуральное число p, не превосходящее некоторой степени q^k произвольным образом фиксированного натурального числа q, единственным образом представляется в виде

$$p = a_0 + a_1q + \cdots + a_{k-1}q^{k-1}\,.$$

Пример: при $q = 10$ это позволяет записать всякое $n \in \mathbb{N}$, $n < 10^k$, k-значным десятичным числом.

3.3. Поле частных, подобное $k(x_1, x_2, \dots, x_n)$ или $\mathbb{Q}$, можно построить исходя из любого *целостного* коммутативного кольца K. А именно, обозначим через a/b $(a, b \in K)$ класс возможных пар
$$\{(c, d) \in K \times K : \; ad = bc\} .$$
Эти классы разбивают $K \times K$ в объединение непересекающихся подмножеств, ибо если (c, d) входит и в a_1/b_1 и в a_2/b_2, то вычитая из равенства $a_1db_2 = b_1cb_2$ (полученного умножением обеих частей $a_1d = b_1c$ на b_2) аналогичное равенство $a_2db_1 = b_2cb_1$, получим $d(a_1b_2 - b_2a_1) = 0$, что ввиду целостности K влечёт равенство $a_1b_2 = b_2a_1$, означающее, что классы a_1/b_1 и a_2/b_2 совпадают.

Фактор-множество $K \times K$, состоящее из описанных только что классов a/b называется *полем частных* целостного коммутативного кольца K. Операции в этом поле определяются, как и ранее, правилами (8-1).

Задача 8.21. Проверьте, что опреации определены корректно и удовлетворяют всем аксиомам поля.

3.3.1. Пример: поле рядов Лорана. Пусть в предыдущей конструкции $K = k[[t]]$ будет кольцом формальных степенных рядов над полем k. Поле частных обозначается в этом случае $k((t))$. Напомню (см. лекцию 2), что каждый элемент $f(t) \in k[[t]]$ единственным образом представим в виде $f(t) = t^d f_0(t)$, где $d \in \mathbb{N}$, а $f_0(t)$ имеет ненулевой свободный член, и стало быть, обратим в $k[[t]]$. Поэтому всякий элемент $f/g \in k((t))$ может быть (также единственным способом) записан в виде $f(t)/g(t) = t^m r_0(t)$, где $m \in \mathbb{Z}$, а $r_0(t)$ – обратимый степенной ряд. Таким образом, всякий $l \in k((t))$ представляется рядом $l(t) = \sum\limits_{\nu \geq \nu_{\min}} a_\nu t^\nu$ по целым степеням переменной, в котором допускается лишь конечное число отрицательных степеней. Такие ряды называются *степенными рядами Лорана*.

Задача 8.22. Убедитесь непосредственным вычислением, что степенные ряды Лорана составляют поле.

Итак, поле частных кольца $k[[t]]$ изоморфно полю рядов Лорана.

3.4. Факториальность кольца многочленов. Пусть A – факториальное кольцо, и K – его поле частных. Внимательный анализ доказательств из лекции 3 показывает, что между разложением на множители в кольце $A[x]$ и разложением на множители в кольце $K[x]$ должна быть точно такая же связь как и в случае $A = \mathbb{Z}$, $K = \mathbb{Q}$.

Действительно, для любого набора элементов $a_1, a_2, \dots, a_n \in A$ можно определить их наибольший общий делитель *НОД* $(a_1, a_2, \dots, a_n)$ как максимальную общую часть разложений всех этих элементов на простые множители (как и в кольце главных идеалов, такой *НОД* будет определён однозначно с точностью до умножения на обратимые элементы кольца). После этого мы также как в лекции 3 можем определить *содержание* $\mathrm{cont}\,(f)$ многочлена $f \in A[x]$ и дословно теми же рассуждениями доказать лемму Гаусса.

Задача 8.23. Докажите, что:

(i) для любых двух многочленов $f, g \in A[x]$ выполнено равенство
$$\mathrm{cont}(fg) = \mathrm{cont}(f) \cdot \mathrm{cont}(g) ;$$

(ii) любой многочленов $f(x) \in K[x]$ представляется в виде $\dfrac{\widehat{f}(x)}{a}$, где $a \in A$ и $\widehat{f}(x) \in A[x]$ – многочлен содержания 1, причём a и $\widehat{f}$ определяются по f однозначно с точностью до умножения на обратимый элемент кольца A;

(iii) всякий многочлен $f \in A[x]$, который раскладывается в $K[x]$ в произведение двух многочленов меньшей степени, будет и в $A[x]$ раскладываться в произвеедение двух многочленов тех же степеней.

Таким образом, множество неприводимых элементов кольца $A[x]$ состоит из неприводимых констант из A и неприводимых над полем K многочленов содержания 1. Из этого вытекает

3.4.1. Предложение. *Неприводимые элементы $A[x]$ просты.*

Доказательство. Надо проверить, что если gh делится на неприводимый многочлен f, то либо g либо h делится на f.

Если $f \equiv p = \text{const} \in A$ — неприводимое число, то оно просто вследствие факториальности A, и либо $\text{cont}(g)$, либо $\text{cont}(h)$ делится на p (ибо $\text{cont}(g)\text{cont}(h) = \text{cont}(gh)$ делится на p). Тем самым, p выносится из всех коэффициентов одного из многочленов, что и требовалось.

Если $f(x) \in A[x]$ – неприводимый над K многочлен содержания 1, то либо g, либо h делится на f в $K[x]$ (ибо неприводимые многочлены над полем просты). Если это, к примеру, g, то записывая частное в виде $\dfrac{g(x)}{f(x)} = \dfrac{q(x)}{a}$, где $q(x) \in A[x]$ – многочлен содержания 1, а $a \in A$, получим

$$a \cdot g(x) = f(x) \cdot q(x)\ .$$

Сравнивая содержание обеих частей по лемме Гаусса находим, что a – обратим в A (ибо $a\,\text{cont}\, g = \text{cont}\, f\,\text{cont}\, q = 1$), и значит, $g/f \in A[x]$, что и требовалось.

□

3.4.2. Следствие. *Кольцо многочленов над факториальным кольцом факториально.*

□

По индукции отсюда немедленно вытекает

3.4.3. Следствие. *Кольцо многочленов от n переменных над факториальным кольцом факториально.*

□

§4. Разложение алгебраической функции в дробно-степенной ряд

4.1. Неявные алгебраические функции. Под *неявной формальной алгебраической функцией* от переменной t мы будем понимать корень $x(t)$ многочлена

$$f_t(x) = a_0(t)x^n + a_1(t)x^{n-1} + \cdots + a_{n-1}(t)x + a_n(t)$$

коэффициенты которого являются формальными степенными рядами от t.

Если t пробегает какую-либо область в $\mathbb{R}$ или $\mathbb{C}$ и ряды $a_i(t)$ сходятся в этой области, то корень $x(t)$ представляет "настоящую" (мноозначную) функцию от t. Простейшими примерами таких функций являются, скажем, $x(t) = \sqrt{1+t^2}$ и $x(t) = \dfrac{1}{1+t^2}$, представляющие собой, соответственно, корени квадратного многочлена $x^2 - a(t)$ и линейного многочлена $a(t)x - 1$, где $a(t) = 1 + t^2$.

Таким образом, функции, которые мы собираемся рассматривать, есть алгебраические функции наиболее общего вида, влючающие в себя, в частности, рациональные функции и радикалы. Остаток лекции будет посвящён тому, чтобы показать, что всякая такая функция может быть разложена в формальный степенной рядом Лорана от $\sqrt[d]{t}$ для подходящего $d \in \mathbb{N}$. Этот ряд называется *рядом Пюизо* рассматриваемой алгебраической функции. Интуитивное значение этого результата может быть выражено словами "всякая функция, записанная формулой, формально раскладывается в дробно-степенной ряд".

Задача 8.24. Разложите $\sqrt{1+t+t^2}$ и $1/(1+t+t^2)$ в формальные степенные ряды по натуральным степеням t

Сразу оговоримся, что мы не будем здесь заниматься вопросами сходимости и остановимся только на алгебраической стороне дела: существовании такого ряда $\vartheta(\sqrt[d]{t})$, что после подстановки $x = \vartheta(t)$ в многочлен $a_0(t)x^n + a_1(t)x^{n-1} + \cdots + a_n(x)$ получится тождественно нулевой ряд от $\sqrt[d]{t}$. Точное утверждение таково:

4.2. Теорема. *Пусть k – алгебраически-замкнутое поле характеристики нуль и пусть $K = k((t))$ – поле рядов Лорана над k. Тогда для любого многочлена $f(x) \in K[x]$,*

$$f(x) = a_0(t)x^n + a_1(t)x^{n-1} + \cdots + a_n(x)$$

существует такой ряд $\vartheta(s) \in k((s))$ и такое число $d \in \mathbb{N}$, что в поле $k((s))$ выполнено тождество

$$f(\vartheta(s)) = a_0(s^d)\vartheta(s)^n + a_1(s^d)\vartheta(s)^{n-1} + \cdots + +a_n(s^d) \equiv 0\ .$$

4.3. Доказательство теоремы основывается на следующем фундаментальном факте, известном как *лемма Гензеля.*

4.3.1. Лемма. *Пусть k — любое поле, а*

$$G(t,x) = x^m + g(t)_1 x^{m-1} + \cdots + g(t)_{m-1}x + g(t)_m \in k[[t]][x]$$

– многочлен от x со старшим коэффициентом единица и прочими коэффициентами из кольца формальных степенных рядов $k[[t]]$. Если многочлен

$$G(0,x) = x^m + g(0)_1 x^{m-1} + \cdots + g(0)_{m-1}x + g(0)_m \in k[x]$$

раскладывается в $k[x]$ на два взаимно простых множителя $a(x)$ и $b(x)$ с $\deg a \geq 1$ и $\deg b \geq 1$, то $G(t,x)$ раскладывется на два взаимно-простых множителя $A(t,x)$ и $B(t,x)$ в $k[[t]][x]$, причём $\deg A \geq 1$, $\deg B \geq 1$ и $A(0,x) = a(x)$, $B(0,x) = b(x)$.

Доказательство. Воспользуемся методом неопределенных коэффициентов, т. е. будем искать $A(t,x)$ и $B(t,x)$ в виде

$$\begin{aligned} A(t,x) &= a_0(x) + a_1(x)t + a_2(x)t^2 + \cdots \\ B(t,x) &= b_0(x) + b_1(x)t + b_2(x)t^2 + \cdots\ , \end{aligned}$$

где $a_i(x)$ и $b_i(x)$ – многочлены из $k[x]$ степени *не больше, чем* $\deg(G) - 1$. В качестве $a_0(x)$ и $b_0(x)$ выберем $a(x)$ и $b(x)$, дающие разложение $G(0,x)$ из условия леммы. Для нахождения остальных a_i, b_i переразложим $G(t,x)$ по степеням t

$$G(t,x) = g_0(x) + g_1(x)t + g_2(x)t^2 + \cdots \quad ,$$

и приравнивая коэффициенты при одинаковых степенях t в равенстве $G(t,x) = A(t,x)B(t,x)$, получим рекурентную формулу

$$a_0(x)b_k(x) + b_0(x)a_k(x) = g_k(x) - \sum_{i+1}^{k-1} a_i(x)b_{k-i}(x) \ ,$$

позволяющую по индукции найти $a_k(x)$ и $b_k(x)$. Действительно, многочлен

$$r(x) = g_k(x) - \sum_{i+1}^{k-1} a_i(x)b_{k-i}(x)$$

в правой части зависит только от предыдущих a_i, b_i с $i < k$, многочлены a_0 и b_0 взаимно просты по условию леммы, и стало быть a_k есть единственный многочлен степени $< \deg a_0$, представляющий класс $[r][b_0]^{-1} \bmod a_0 \in k[x]/(a_0(x))$, а b_k есть единственный многочлен степени $< \deg b_0$, представляющий класс $[r][a_0]^{-1} \bmod b_0 \in k[x]/(b_0(x))$.
□

4.3.2. Окончание доказательства теоремы. Вернемся к полю $K = k((t))$ формальных рядов Лорана над алгебраически замкнутым полем k характеристики нуль, и пусть

$$f_t(x) = a_0(t)x^n + a_1(t)x^{n-1} + \cdots + a_n(x) \in K[x]$$

– какой-либо многочлен над K. Мы собираемся найти его корень, возможно после некоторой параметризации $t = s^d$.

Заметим прежде всего, что достаточно рассмотреть только случай, когда старший коэффициент a_0 многочлена f равен единице, а остальные коэффициенты лежат в кольце $k[[t]]$. Действительно, после умножения обеих частей уравнения $f(x) = 0$ на достаточно большую степень t^N, можно считать, что все $a_i \in k[[t]]$, и затем, умножив обе части на $a_0(x)^{n-1}$ и сделав линейную замену $z = a_0(t)x$, получить на z уравнение со старшим коэффициентом 1, умение решать которое в поле K равносильно умению решать в поле K исходное уравнение.

Итак, пусть $f_t(x) = x^n + a_1(t)x^{n-1} + \cdots + a_n(x) \in k[[t]][x]$. Поскольку линейные уравнения (отвечающие $n = 1$) решаются над $K = k((t))$ без проблем, нам достаточно (благодаря индукции по n) разложить f в $k[[t]][x]$ на множители строго меньшей степени. Я утверждаю, что это всегда возможно, может быть, после некоторой замены параметра $t = s^d$.

В самом деле, по лемме Гензеля достаточно уметь раскладывать $f_0(x) = f_t(x)|_{t=0}$ на два нетривиальных взаимно простых множителя в $k[x]$. Поскольку поле k алгебраически замкнуто (и стало быть, каждый многочлен является произведением линейных), такое разложение невозможно только в случае, когда $f_0(x) = (x - \alpha)^n$ является чистой степенью линейного. Это можно исправить подходящим сдвигом переменной x и сменой параметра $t = s^d$.

Действительно, заменяя x на $x - a_1(t)/n$, можно считать, что $f_t(x)$ не содержит члена с $x^n - 1$. Если при при таком сдвиге исчезнут и все меньшие степени, т. е. $f_t(x)$ превратится в x^n, то мы получаем тривиальное решение $x = \vartheta(t) \equiv 0$ и больше делать нечего. Если же после сдвига останутся какие-то ненулевые коэффициенты

$$a_m(t) = \alpha_{\nu_m} t^{\nu_m} + \text{члены большей степени по } t \ ,$$

то мы выберем наименьшую из всех дробей $\frac{\alpha_{\nu_m}}{m}$ (ν_m пробегает младшие степени всех ненулевых рядов a_m) и рассмотрим её несократимую запись p/q. Отметим, что по построению

$q\nu_m \geq pm$ при всех $m \geq 2$. Сделаем теперь замену $t = s^q$, $x = s^p y$. Получим

$$\begin{aligned} p_t(x) &= x^n + \sum_{m=2}^{n} (\alpha_{\nu_m} t^{\nu_m} + \cdots) x^{n-m} = \\ &= s^{pn} y^n + \sum_{m=2}^{n} s^{p(n-m)+q\nu_m} (\alpha_{\nu_m} + \cdots) y^{n-m} = \\ &= s^{np} \Big(y^n + \sum_{m=2}^{n} s^{q\nu_m - pm} (\alpha_{\nu_m} + \cdots) y^{n-m} \Big) \end{aligned}$$

где все ряды-коэффициенты справа содержат неотрицательные степени s (поскольку $q\nu_m \geq pm$), и хотя бы один из них (у которого $q\nu_m = pm$) имеет ненулевой свободный член. а стало быть гарантированно не занулится при $s = 0$. Таким образом, после сокращения на s^{pn} мы получаем на y уравнение, правая часть которого не является чистой степенью линейной формы при $s = 0$, поскольку будет содержать при $s = 0$ некий член y^i с $i < n$, но не будет содержать y^{n-1} (над полем характеристики нуль $(y - \alpha)^n$ либо совпадает с y^n (при $a = 0$) либо содержит *все без исключения* члены y^m с $0 \leq m \leq n$). Из сказанного ранее вытекает, что это уравнение разрешимо над полем $k((s))$.

Теорема доказана.