

21. Двадцать первая лекция, 11 апреля 2018 г.

21.1. Результат. Рассмотрим два многочлена от одной переменной (над произвольным полем $\mathbb{K}$), степени n и m соответственно:

$$\begin{aligned} f(x) &= a_n x^n + \cdots + a_1 x + a_0; \\ g(x) &= b_m x^m + \cdots + b_1 x + b_0. \end{aligned}$$

Наша ближайшая задача — определить, имеют ли эти многочлены общий сомножитель.

Сначала дадим на этот вопрос «малоинформативный» ответ. Предположим, что общий множитель у f и g есть: $f = f_1 h$, $g = g_1 h$, где $\deg h > 0$. Это значит, что у них имеется общее кратное степени строго меньшей, чем $m + n$. Это кратное есть $f_1 g_1 h$. При этом «дополнительные множители», на которые надо домножить f и g для того, чтобы его получить, равны g_1 и f_1 соответственно, и их степени не превосходят $m - 1$ и $n - 1$. Напротив, если у f и g нет общих множителей, то их наименьшее общее кратное имеет степень $m + n$, и нельзя найти такие многочлены p и q , где $\deg p < m$, $\deg q < n$, что $fp + gq = 0$.

Тем самым, имеет место следующее предложение:

ПРЕДЛОЖЕНИЕ 21.1. *Многочлены $f(x)$ и $g(x)$, где $\deg f = n$, $\deg g = m$, имеют общий множитель тогда и только тогда, когда найдутся такие многочлены $p(x)$ и $q(x)$, не равные одновременно нулю, где $\deg p(x) \leq m - 1$, $\deg q(x) \leq n - 1$, что $f(x)p(x) + g(x)q(x) = 0$.*

Попробуем интерпретировать это условие как-то ещё. Выпишем многочлены $p(x)$ и $q(x)$:

$$\begin{aligned} p(x) &= p_{m-1} x^{m-1} + \cdots + p_1 x + p_0; \\ q(x) &= q_{n-1} x^{n-1} + \cdots + q_1 x + q_0. \end{aligned}$$

Запишем в явном виде условие из предложения 21.1:

$$\begin{aligned} f(x)p(x) + g(x)q(x) &= (a_n p_{m-1} + b_m q_{n-1})x^{m+n-1} + \\ &+ (a_{n-1} p_{m-1} + a_n p_{m-2} + b_{m-1} q_{n-1} + b_m q_{n-2})x^{m+n-2} + \cdots + a_0 p_0 + b_0 q_0 = 0. \end{aligned}$$

Условие равенства многочлена степени $m + n - 1$ нулю — это система из $m + n$ линейных однородных уравнений на неизвестные $p_{m-1}, \dots, p_0, q_{n-1}, q_0$. Искомые многочлены $p(x)$ и $q(x)$ существуют тогда и только тогда, когда у этой системы есть ненулевое решение, т.е. когда матрица системы вырождена. Определитель этой матрицы называется *результантом* многочленов $f(x)$ и $g(x)$ и обозначается $\text{Res}(f, g)$. Выпишем его явно:

$$\text{Res}(f, g) = \begin{vmatrix} a_n & & & & b_m & & & \\ a_{n-1} & a_n & & & b_{m-1} & b_m & & \\ \vdots & a_{n-1} & \ddots & & \vdots & b_{m-1} & \ddots & \\ a_0 & \vdots & \ddots & a_n & b_0 & \vdots & \ddots & b_m \\ & a_0 & & a_{n-1} & & b_0 & & b_{m-1} \\ & & \ddots & \vdots & & & \ddots & \vdots \\ & & & a_0 & & & & b_0 \end{vmatrix}$$

Мы доказали следующую теорему.

ТЕОРЕМА 21.2. *Многочлены $f(x)$ и $g(x)$ имеют общий множитель тогда и только тогда, когда их результат $\text{Res}(f, g)$ равен нулю.*

СЛЕДСТВИЕ 21.3. Пусть многочлены $f(x)$ и $g(x)$ имеют общий корень. Тогда $\text{Res}(f, g) = 0$.

21.2. Другие формулы для результата. Предположим, что многочлены $f(x)$ и $g(x)$ раскладываются на линейные множители:

$$\begin{aligned} f(x) &= a_n(x - t_1) \dots (x - t_n); \\ g(x) &= b_m(x - u_1) \dots (x - u_m). \end{aligned}$$

Коэффициенты a_k и b_k выражаются через корни этих многочленов:

$$a_k = a_n(-1)^{n-k} e_{n-k}(t_1, \dots, t_n), \quad b_k = b_m(-1)^{m-k} \tilde{e}_{m-k}(u_1, \dots, u_m), \quad (*)$$

где e и $\tilde{e}$ — элементарные симметрические многочлены от n и m переменных соответственно. Также полезно заметить, что $\text{Res}(f, g)$ является однородным многочленом от a_i степени m и от b_j степени n .

ПРЕДЛОЖЕНИЕ 21.4. Имеют место равенства

$$\text{Res}(f, g) = a_n^m b_m^n \prod_{i=1}^n \prod_{j=1}^m (t_i - u_j) = a_n^m \prod_{i=1}^n g(t_i) = (-1)^{mn} b_m^n \prod_{j=1}^m f(u_j).$$

ДОКАЗАТЕЛЬСТВО. Последние два равенства очевидно следуют из вида разложения $f(x)$ и $g(x)$ на линейные множители. Докажем первое равенство.

Во-первых, из равенств $(*)$ следует, что $\text{Res}(f, g)$ как многочлен от a_n, b_m, t_i, u_j делится на $a_n^m b_m^n$. Кроме того, $\text{Res}(f, g)$ обращается в нуль, если многочлены f и g имеют общий корень, т.е. если $t_i = u_j$ при каких-то i, j . Поэтому $\text{Res}(f, g)$ делится на любую из разностей $t_i - u_j$, а значит, и на их произведение. Мы доказали, что $\text{Res}(f, g)$ делится на $a_n^m b_m^n \prod_{i=1}^n \prod_{j=1}^m (t_i - u_j)$.

Далее, заметим, что оба эти выражения имеют степень m как многочлены от $a_0, \dots, a_n$: про результат это, как было сказано выше, следует из его явного вида, а про правую часть это верно в силу того, что она равна $(-1)^{mn} b_m^n \prod_{j=1}^m f(u_j)$, а каждый из сомножителей $f(u_j)$ линейен как многочлен от a_i . По тем же соображениям они оба имеют степень n как многочлены от $b_0, \dots, b_m$. Следовательно, эти выражения получаются друг от друга домножением на элемент основного поля $\mathbb{K}$.

Для завершения доказательства заметим, что оба эти выражения как многочлены от a_i и b_j содержат одночлен $a_n^m b_m^n$ с коэффициентом 1. Поэтому они равны. $\square$

21.3. Дискриминант. Рассмотрим многочлен $f(x)$, раскладывающийся на линейные множители:

$$f(x) = a_n(x - t_1) \dots (x - t_n).$$

ОПРЕДЕЛЕНИЕ 21.5. Дискриминант многочлена f — это многочлен

$$D(f) = a_n^{2n-2} \prod_{i < j} (t_i - t_j)^2 = \left[a_n^{n-1} \prod_{i < j} (t_i - t_j) \right]^2.$$

Из определения ясно, что дискриминант обращается в нуль тогда и только тогда, когда среди корней многочлена $f(x)$ есть совпадающие.

Далее, дискриминант является симметрическим многочленом от $t_1, \dots, t_n$, поэтому это многочлен от $a_0, \dots, a_{n-1}, a_n$ и a_n^{-1} . (Контрольный вопрос: зачем здесь a_n^{-1} ?) Найдём этот многочлен. Для этого нам потребуется понятие *производной* многочлена.

ОПРЕДЕЛЕНИЕ 21.6. Пусть $f(x) = a_n x^n + \dots + a_1 x + a_0 \in K[x]$ — многочлен. Его *производная* — это многочлен $f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + 2 a_2 x + a_1 \in K[x]$.

ЗАМЕЧАНИЕ 21.7. Это определение производной многочлена является чисто алгебраическим (в отличие от того, которое давалось в курсе математического анализа — в последнем участвовало понятие предельного перехода). Поэтому имеет смысл говорить о производной многочлена над произвольным полем, в том числе ненулевой характеристики. В отличие, скажем, от вещественной или комплексной ситуации, в характеристике p бывают многочлены, имеющие нулевую производную, но отличные от констант — например, x^p .

УПРАЖНЕНИЕ 21.8. Докажите, что сумму и произведение многочленов можно дифференцировать по правилам, известным из матанализа: $(f+g)' = f' + g'$ и $(fg)' = f'g + fg'$.

ПРЕДЛОЖЕНИЕ 21.9. *Дискриминант многочлена пропорционален результату его самого и его производной:*

$$D(f) = (-1)^{n(n-1)/2} a_n^{-1} \operatorname{Res}(f, f').$$

ДОКАЗАТЕЛЬСТВО. Продифференцируем производную многочлена по правилу Лейбница:

$$f'(x) = \left(a_n \prod_{i=1}^n (x - t_i) \right)' = a_n \sum_{i=1}^n \prod_{j \neq i} (x - t_j).$$

Особенно хорошо выглядит выражение для производной f' в корне t_i многочлена f : там все слагаемые в последней сумме, кроме i -го, обращаются в нуль:

$$f'(t_i) = a_n \prod_{j \neq i} (t_i - t_j).$$

Воспользовавшись предложением 21.4, получим:

$$\begin{aligned} \operatorname{Res}(f, f') &= a_n^{2n-1} \prod_{i=1}^n \prod_{j \neq i} (t_i - t_j) = \\ &= a_n (-1)^{n(n-1)/2} a_n^{2n-2} \prod_{i < j} (t_i - t_j)^2 = a_n (-1)^{n(n-1)/2} D(f), \end{aligned}$$

что и требовалось доказать. □

УПРАЖНЕНИЕ 21.10. Вычислите дискриминанты многочленов $ax^2 + bx + c$ и $x^3 + px + q$ (любой кубический многочлен можно линейной заменой привести к такому виду).

E-mail address: esmirnov@hse.ru