9. Девятая лекция, 8 ноября 2022 г.

9.1. **Результант.** Рассмотрим два многочлена от одной переменной над произвольным факториальным кольцом A, степени n и m соответственно:

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

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

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

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

Запишем в явном виде условие из предложения 9.1:

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

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 $\mathrm{Res}(f,g)$. Выпишем его явно:

$$\mathrm{Res}(f,g) = \begin{vmatrix} a_n & & & & b_m & & & \\ a_{n-1} & a_n & & & b_{m-1} & b_m & & \\ \vdots & a_{n-1} & \ddots & & \vdots & b_{m-1} & \ddots & \\ a_1 & \vdots & \ddots & a_n & b_1 & \vdots & \ddots & b_m \\ a_0 & a_1 & & a_{n-1} & b_0 & b_1 & & b_{m-1} \\ & a_0 & \ddots & \vdots & & b_0 & \ddots & \vdots \\ & & \ddots & a_1 & & & \ddots & b_1 \\ & & & a_0 & & & & b_0 \end{vmatrix}$$

Мы доказали следующую теорему.

Теорема 9.2. *Многочлены $f(x)$ и $g(x)$ имеют общий множитель тогда и только тогда, когда их результант* $\mathrm{Res}(f,g)$ *равен нулю.*

Следствие 9.3. *Пусть многочлены $f(x)$ и $g(x)$ имеют общий корень. Тогда* $\mathrm{Res}(f,g) = 0$.

9.2. **Другие формулы для результанта.** Предположим, что многочлены $f(x)$ и $g(x)$ раскладываются над исходным кольцом A 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 по формулам Виета:

$$a_k = a_n(-1)^{n-k}\sigma_{n-k}(t_1,\dots,t_n), \quad b_k = b_m(-1)^{m-k}\widetilde{\sigma}_{m-k}(u_1,\dots,u_m), \tag{1}$$

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

Предложение 9.4. *Справедливы равенства*

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

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

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

Для завершения доказательства заметим, что оба эти выражения как многочлены от a_i и b_j содержат одночлен $a_n^m b_0^n$ с коэффициентом 1. Поэтому они равны. □

9.3. **Кратные корни многочленов и производная.**

Определение 9.5. Пусть $f(x) \in A[x]$ — некоторый многочлен. Элемент $a \in A$ называется *корнем* многочлена $f(x)$ *кратности* k, если $f(x)$ представим в виде

$$f(x) = (x-a)^k g(x),$$

где $g(a) \neq 0$.

Для работы с кратными корнями полезно ввести определение производной многочлена.

Определение 9.6. Пусть $f(x) = a_n x^n + \dots + a_1 x + a_0 \in A[x]$ — многочлен. Его *производная* — это многочлен $f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \dots + 2a_2 x + a_1 \in A[x]$.

Замечание 9.7. 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 9.8. Докажите, что сумму и произведение многочленов можно дифференцировать по правилам, известным из матанализа: $(f+g)' = f'+g'$ (линейность) и $(fg)' = f'g + fg'$ (правило Лейбница).

Справедливо следующее предложение.

Предложение 9.9. *Корень $a \in A$ многочлена $f(x)$ имеет кратность не менее 2 тогда и только тогда, когда a также является корнем производной $f'(x)$. Более общим образом, корень имеет кратность не менее k тогда и только тогда, когда $f(a) = f'(a) = \dots = f^{(k-1)}(a) = 0$.*

Доказательство. Докажем первое утверждение. Пусть a — корень кратности не менее 2. Тогда $f(x) = (x-a)^2 g(x)$. Продифференцировав это произведение по правилу Лейбница, получим

$$f'(x) = (x-a)^2 g'(x) + 2(x-a)g(x).$$

Ясно, что в таком случае a является также корнем $f(x)$. Обратное утверждение доказывается аналогично: если a — корень кратности 1, то $f(x) = (x-a)g(x)$, где $g(a) \neq 0$, и тогда

$$f'(x) = g(x) + (x-a)g'(x),$$

откуда $f'(a) = g(a) \neq 0$.

Утверждение о произвольной кратности получается из первого утверждения по индукции; доказательство оставляется читателю в качестве несложного упражнения. □

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

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

Определение 9.10. *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.

Предложение 9.11. *Дискриминант многочлена пропорционален результанту 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 9.4, получим:

$$\operatorname{Res}(f, f') = a_n^{2n-1} \prod_{i=1}^{n} \prod_{j \neq i}(t_i - t_j) =$$

$$= a_n(-1)^{n(n-1)/2} a_n^{2n-2} \prod_{i<j}(t_i - t_j)^2 = a_n(-1)^{n(n-1)/2} D(f),$$

что и требовалось доказать.

□